Ph.D. Dissertation in Engineering

Cloud Federation Formation: Enabling Factors, Requirements, Challenges, and Current Trends with an Emphasis on Institutional Trust and Distributed Trust Evaluation

클라우드 연합 형성: 기관 신뢰도와 분산 신뢰도 평가를 통한 요인, 요구사항, 과제 및 현재 동향 지원

August 2023

Graduate School of Seoul National University

Technology Management, Economics, and Policy Program

Weldemehret Yodit Gebrealif

Cloud Federation Formation: Enabling Factors, Requirements, Challenges, and Current Trends with an Emphasis on Institutional Trust and Distributed Trust Evaluation

지도교수 **Jörn Altmann**

이 논문을 공학박사 학위 논문으로 제출함
2023 년 8 월

서울대학교 대학원
협동과정 기술경영경제정책 전공

Weldemehret Yodit Gebrealif

웰데메레 요딧 게브렐리프의 공학박사학위 논문을 인준함

2023 년 **8** 월

위 원 장 구윤모 (인)

부위원장 Jörn Altmann (인)

위 원 Bernhard Egger (인)

위 원 Konstantinos Tserpes (인)

위 원 이울림 (인)

Abstract

Cloud Federation Formation: Enabling Factors, Requirements, Challenges, and Current Trends with an Emphasis on Institutional Trust and Distributed Trust Evaluation

Weldemehret Yodit Gebrealif
Technology Management, Economics, and Policy Program
College of Engineering
Seoul National University

Cloud computing is a rapidly growing industry offering numerous benefits to customers, including access to emerging technologies, innovation, and scalability. However, the market is largely dominated by a few major players, limiting the competitiveness of small and medium-sized cloud providers. To effectively compete, small and medium-sized cloud providers need to adopt a multi-cloud strategy, utilizing multiple cloud providers for different purposes. One way to implement a multi-cloud strategy is through cloud federation, which allows cloud providers

to buy and sell services from other providers on demand to increase reliability, reduce cost and energy consumption, and provide easy scaling up of resources. This dissertation presents a compelling and comprehensive investigation into the critical phase of cloud federation formation, encompassing two essential studies. The first study conducts a systematic literature review to explore the enabling factors, requirements, challenges, and current trends in cloud federation formation. This review serves as a strong foundation for the subsequent study, which proposes an innovative Institutional Quality-Aware Trusted Cloud Federation Formation approach. The Institutional Quality-Aware Trusted Cloud Federation Formation method is designed to address the complexities and uncertainties involved in forming cloud federations. A novel cloud federation overall architecture and a novel cloud federation formation algorithm is introduced, while also emphasizing a two-stage trust evaluation process for cloud service providers to select reliable partners.

In this study, six research questions were formulated to investigate cloud federation formation comprehensively. The systematic literature review addressed the first four research questions and successfully identified 16 enabling factors, 17 requirements, and 18 major challenges related to cloud federation formation. Among the enabling factors, resource

provisioning and flexibility emerged as the most extensively discussed, while legal issues and regulatory compliance were relatively underexplored.

Regarding requirements, trust and reputation among cloud service providers were the most extensively studied, emphasizing their significance in forming successful cloud federations. Additionally, cloud federation stability emerged as a prominent challenges that received substantial attention in the reviewed studies. Notably, the most commonly used research trends were game theory and set theory, and the proposed solutions predominantly revolved around algorithmic approaches and mathematical models.

The second study aimed to address the last two research questions and presented institutional quality-aware trusted cloud federation formation approaches. This innovative approach utilized a two-stage trust evaluation process. The first stage involved computing cloud service provider trust and institutional trust to determine the cloud service provider global trust. In the second stage, trust was aggregated based on direct and indirect feedback from cloud service providers and users. By incorporating a confidence score for feedback aggregation, the approach effectively mitigated the risks of false positive and false negative feedback. The

proposed model was subjected to evaluation through two experiments, demonstrating its effectiveness in identifying trusted potential partners for forming a coalition based on trust. These findings highlight the importance of trust-aware approaches in cloud federation formation and contribute valuable insights to enhance the reliability and success of multi-cloud strategies. Furthermore, the research provides a solid basis for fostering collaboration between cloud service providers and enables small and medium-sized providers to effectively compete with dominant players in the cloud computing market.

Keywords: Trusted Cloud Federation, Institutional Quality, Trust, Regulatory Quality, Cloud federation formation, Cloud coalition formation, Cooperation formation

Student Number: 2020-32099

Table of Contents

List of Figures

List of Tables

List of Abbreviations

APIs: Application Program Interfaces

AWS: Amazon Web Service

BCRs: Binding Corporate Rules

CC: Control of Corruption

CCPA: California Consumer Privacy Act

CF: Cloud Federation

CFF: Cloud Federation Formation

CP: Cloud Provider

CSP: Cloud Service Providers

EC2: Elastic Compute Cloud

FLA: Federation Level Agreement

GA4GH: Global Alliance for Genomics and Health

GCP: Google Cloud Platform

GDPR: General Data Protection Regulation

GE: Government Effectiveness

IaaS: Infrastructure as a Service

IQ: Institutional Quality

JV: Joint Ventures

KBT: Knowledge-Based Theory

KPI: Key Performance Indicator

NIC: Network Interface Card

NIST: National Institute of Standards and Technology

NSF: National Science Foundation

PaaS: Platform As A Service

PS: Political Stability no violence

QoS: Quality of Service

RBV: Resource-Based View

RL: Rule of Law

RQ: Regulatory Quality

S3: Simple Storage Service

SaaS: Software As A Service

SCCs: Standard Contractual Clauses

SLA: Service Level Agreement

SLR: Systematic Literature Review

TCB: Trusted Cloud Broker

TCE: Transaction Cost Economics

TU: Transferable Utility

VM: Virtual Machine

VoA: Voice of Accountability

Chapter 1. Introduction

1.1. Background and Motivation

According to the recent reports by Dgtl Infra, (Mary, 2023, p. 10) the top 10 cloud service providers' globally in 2023 control ~80% of the cloud market. Furthermore, the report also states that the worldwide end-user spending on public cloud service is forecast to grow 21.7% to a total of $579.3 billion in 2023 up from $491 billion in 2022 and also forecasted to $725 billion by 2024 (STAMFORD, Conn, 2023). This is driven by the adoption of emerging technologies like generative AI, Web3, and the Meta verse (STAMFORD, Conn, 2023). While the top 10 cloud providers control most of the market share, there are numerous small and medium-sized cloud providers in the market that operate regionally. Some of these small and medium-sized cloud service providers' are:

- **China**: Badiu AI Cloud, JD Cloud, UCloud (Mary, 2023, p. 10)
- **Europe**: Bleu (Orange and Capgemini), Hetzner, Leaseweb (Mary, 2023, p. 10)
- **Japan and Korea**: Fujitsu, NAVER Cloud, KT Cloud (Mary, 2023, p. 10)
- **Africa**: Telecloud, Web4Africa, Layer3Cloud, Cloudafrica

As the emerging technology adoption increase, cloud service providers provide a customer with cutting-edge innovation and valuable service. So for small providers to expand their capability and to be able to provide cutting-edge innovation and service, numerous cloud providers are expected to adopt an intercloud strategy by 2023, which means using multiple cloud providers for different purposes (Matthew Vulpis, 2023). Cloud federation as a part of an intercloud strategy, allows cloud providers to buy and sell services on demand, increase reliability, reduce cost and energy consumption, and provide easy scaling up of resources. As businesses and individuals increasingly rely on cloud computing services to fulfill their computing needs, it is no wonder that cloud computing services are growing rapidly. However, the current market structure, which consists of a limited number of large cloud service providers, presents a risk of market concentration and lock-in, which may lead to higher costs and reduced innovation over time due to a lack of competition.

Furthermore, the existing company that offers cloud federation service offers the service partner with the large cloud providers. For example, VMware offers enterprise federation to activate single sign-on for users in multiple enterprises and it partners with various cloud providers such as AWS, Azure, Google Cloud, IBM Cloud, Oracle Cloud, and more(Sotiriadis et al., 2014; What Is Enterprise Federation and How

Does It Work with VMware Cloud Services, 2022). Similarly, Azure Arc is a service that enables clients to manage and govern resources across different cloud providers and platforms such as AWS, Google Cloud, VMware, Kubernetes, and more(Buchanan & Joyner, 2022; Nocentino & Weissman, 2021).

Table 1.1: Top 10 public cloud service providers and their market coverage as of 2023 (Mary, 2023, p. 10)

# (Rank)	Cloud Service Provider	Market share	Region	Availability Zones
1	Amazon Web Service (AWS)	34%	26	84
2	Microsoft Azure	22%	60	116
3	Google Cloud Platform (GCP)	9.5%	34	103
4	Alibaba Cloud	6%	27	84
5	Oracle Cloud	2%	38	46
6	IBM Cloud (Kyndryl)	2%	11	29
7	Tencent Cloud	2%	21	65
8	OVHcloud	<1%	13	33
9	DigitalOceab	<1%	8	14
10	Linode (Akamai)	<1%	11	11

This shows that the companies who provide cloud federation are only partners with the large provider. The current structures of the cloud federation are not inclusive even though cloud federation was introduced to address the challenges of scalability and elasticity faced by cloud providers, including small and medium-sized cloud providers.

One of the key benefits of cloud federation formation is the ability to leverage multiple cloud service providers' resources and capabilities to deliver better QoS to users. By promoting collaboration and competition among cloud service providers, cloud federation formation can help drive innovation and reduce costs, ultimately leading to better cloud services for businesses and individuals. However, the dominance of a few large cloud service providers in the cloud market presents a significant challenge to the formation of cloud federations among smaller cloud service providers. This is due to the fact that the larger cloud service providers have a strong position in the market and are able to offer competitive pricing, services, and resources that are hard to match for the smaller cloud service providers. Consequently, smaller cloud service providers will have a harder time attracting customers and building their business as a result, which will make it even more difficult for them to invest in the infrastructure and capabilities that will allow them to serve their customers. Due to this, it is crucial for them to join or

establish a cloud federation to take advantage of the cloud market and to get the most benefit from it.

Our research into cloud federation formation is motivated by the need to explore and understand the enabling factors, and requirements to establish cloud federation. In addition, we need to understand the challenges that hinder cloud federation formation with the current trends. The cloud federation formation is a critical stage that determines the success of the entire federation. The formation of a cloud federation must be carefully planned and managed to avoid misalignments, conflicts, and failures, as alliances in other industries do. At this stage, specific criteria and metrics are used for discovering, selecting, and negotiating with the appropriate cloud providers. Participants in this phase collaborate to establish a common vision and strategy, define governance frameworks, build trust, ensure scalability, and establish business relationships. During the formation of a cloud federation, these aspects are crucial since they provide the foundation for its success and pave the way for seamless operations, high-quality services, transparent governance, collaborative partnerships, and long-term competitiveness. Therefore, by identifying the enabling factors, requirements, and challenges and by providing an inclusive, fair, and unbiased trust evaluation strategy, the research can facilitate the formation of cloud federations, which can benefit all types

of cloud providers, users, and the broader economy by enabling greater collaboration and competition among cloud service providers.

We are conducting research that aims to uncover the enabling factors and requirements that influence cloud federation formation, including technical, legal, and governance requirements. As a result, we aim to provide insight into the cloud market for policymakers, regulators, and industry players in order to help them develop effective strategies to encourage greater collaboration and competition in this market, ultimately benefiting users and the economy as a whole. Furthermore, understanding the challenges that hinder cloud federations' formation can help policymakers, regulators, and industry players develop effective strategies to overcome these challenges. For instance, identifying technical requirements, such as interoperability standards and data security protocols, can help ensure the seamless integration of different cloud platforms and enhance the security of cloud services. Similarly, legal and governance requirements, such as data protection laws and regulatory frameworks, can help ensure that cloud federations operate in a fair and transparent manner, promoting trust and collaboration among cloud service providers. Our research aims to provide insights into these requirements to facilitate the formation of efficient and effective cloud federations.

Furthermore, collaboration among cloud providers as a strategic alliance requires a high level of trust between the participants. Trust is a key requirement for any collaboration, including cloud federation, both within and across the country. However, the existing trust evaluation parameters focus primarily on evaluating the trustworthiness of individual cloud service providers, without considering the broader institutional and regulatory environment. The trust evaluation framework for cloud federation formation must consider additional dimensions beyond individual cloud service providers to ensure fair and transparent trust evaluation for cloud federation formation. These dimensions could include the regulation's quality, the rule of law, and the institutional frameworks that govern the cloud market. Evaluating these external factors is critical, especially when there is a lack of information about the individual cloud providers or transparency in assessing cloud providers' trustworthiness. Cloud federations can be formed with reliable providers by establishing a fair and transparent trust evaluation framework that considers organizational and institutional trust, promoting collaboration and competition in the cloud market. By assessing the internal and external trust evaluation factors, the cloud federation trust evaluation framework can identify potential malicious providers and prevent them from participating in the federation. This can help ensure that the federation is established with reliable providers who

can be trusted to deliver high-quality services and uphold the federation's values and objectives.

1.2. Problem Statement

With the growing demand for cloud computing in the highly competitive cloud computing market, small cloud service providers face significant challenges to survive and thrive (F.-K. Wang & He, 2014). Because of concerns about the cost, privacy, data ownership, lock-in, and complexity of commercial cloud providers, the small cloud has emerged as a concept and practice to address these challenges. However, small cloud providers, face resource inelasticity issues due to limited resource capacity. This could lead to decreased customer service quality and revenue loss (Pal et al., 2017). Studies explore the economic feasibility of small cloud providers to federate and will enable them to compete with the big cloud providers (K. Kim et al., 2014). The small cloud providers and the large cloud providers are also attracted to cloud federation due to the potential to offer flexible services (Haile & Altmann, 2015). Moreover, the federation of small and medium cloud providers enables them sharing of computational and storage resources (Panarello et al., 2014). Therefore, Small and medium-sized cloud providers need to have a clear understanding of the consequences of their decisions in order to establish cloud federation successfully (Í. Goiri et al., 2012; Kanwal et al., 2014; Kousiouris et al., 2013; Mashayekhy et

al., 2021). To achieve this, a clear manual or set of standards can be developed to assist cloud providers in making decisions regarding when and under what circumstances cloud federation should be established, as well as identifying the requirements that must be met and challenges that may arise during the formation of the federation.

Several studies have explored and developed a mechanism and game for cloud federation formation including a game-theoretic approach that considers trust, fairness, high reputation, cost, profit, QoS, as well as reliability of cloud providers(Alam et al., 2020; Das et al., 2014; Dhole et al., 2016; Dinachali et al., 2022a; Mashayekhy et al., 2021). Various studies suggest that cloud federation formation can be achieved through different approaches that consider several factors. However, none of the studies clearly address the manual for cloud federation formation and suggest clear proactive and reactive enabling factors which help small and medium cloud providers to assist when making a decision to join a cloud federation. On the other hand, several studies suggest addressing several required factors including the requirement for IaaS (Panarello et al., 2014), Trust evaluation(Ahmed et al., 2019a), legal requirement(Kousiouris et al., 2013), and general requirement(Lee, 2016) for cloud federation. However, these studies do not provide the overall cloud federation formation requirements. In addition, various technologies, innovations, approaches, and strategies

are introduced since these studies. Therefore it is important to provide a manual for cloud providers that will help in the decision-making process by providing a checklist (a reference) of enabling factors, requirements and challenges to be addressed by the cloud providers all in one for effective and efficient decision-making.

On the other hand, there is no doubt that trust evaluation when forming a cloud federation is a critical issue that must be addressed in order to ensure the success of the cloud federation (Ahmed et al., 2019a; Kanwal et al., 2014; Mashayekhy et al., 2021). The main requirement for successful collaboration and resource sharing in a cloud federation is trust between cloud providers (Gupta & Annappa, 2016; Kanwal et al., 2014). However, not all providers are equally trustworthy and reliable, and some may have security or performance issues that can affect the customer data and applications (Kanwal et al., 2014). Therefore it is essential to have and establish trust between cloud providers before establishing and participating in cloud federation (Ahmed et al., 2019a; Kanwal et al., 2014; Mashayekhy et al., 2021). Various models and frameworks have been proposed to address this issue to address the trust evaluation problem (Abusitta et al., 2018b; Ahmed et al., 2019a; Dhole et al., 2016). These existing trust evaluation models have the tendency to favor large-scale cloud providers. One possible reason why the existing trust evaluation models favor big providers is that they rely on a

reputation-based mechanism that aggregates feedback from customers and other peer providers. Reputation-based trust models can be biased towards well-known and popular providers with less feedback and ratings (Ahmed et al., 2019a). Moreover, reputation-based trust evaluation models can be vulnerable to malicious attacks such as collisions, Slade, or dishonest feedback and recommendations that can manipulate the trust score of providers (R. Latif et al., 2021). A few literature tries to address this issue by considering the service level agreement between cloud providers and customers that specify the expected quality of service parameters (Papadakis-Vlachopapadopoulos et al., 2019; Saxena et al., 2019). However, these approaches could not solve all the issues, especially since limited information is available about the cloud service provider.

Therefore, the trust evaluation model for cloud federation that considers various aspects and relevant criteria needs to be developed to address these issues. Furthermore, as cloud federation is a strategic alliance between cloud providers, the trust evaluation process should consider both the formal and informal institutional trust to establish a successful cloud federation. Lastly, this research work will seek a solution for the above-mentioned problems by breaking down the basics of cloud federation formation enabling factors, requirements, challenges,

and current trends. It then later will emphasize the fair and inclusive distributed trust evaluation model for cloud federation formation.

1.3. Research Objectives and Questions

This research is grounded in a strong foundation that aims to provide a clear understanding of the bigger picture within the context of cloud federation formation. We have conducted an extensive systematic literature review to identify and analyze key elements including enabling factors, requirements, and challenges of cloud federation formation. This review helped us establish a comprehensive understanding of the current state of the field and the gaps that exist. Furthermore, our research builds upon this foundation by proposing a novel algorithm and trust evaluation model for partner selection in cloud federation formation.

Therefore, the primary objective of this study is to conduct a systematic review of existing research on cloud federation formation. The purpose is to identify gaps and provide insights for future research to assist researchers in the field. The study will ensure that all relevant research is considered and evaluated and that any gaps or inconsistencies in the literature are identified. In addition, the study aims to analyze the factors that stimulate or motivate cloud federation formation, the requirements that need to be considered when establishing a cloud federation, and the challenges and barriers that cloud service providers may face when forming a cloud federation. The study also aims to

identify and analyze the current trends in cloud federation formation, including the applied theories, methodologies, evaluation metrics, and evaluation environment used to measure the proposed solutions. The ultimate goal is to assist standard organizations throughout cloud federation formation and address the effective and stable cloud federation formation more holistically. To achieve these primary objectives, the study poses four research questions (RQs) that the study attempts to answer by using a systematic literature review. These questions are:

RQ1.1. What are the enabling factors mentioned in the studies that stimulate or motivate cloud federation formation?

RQ1.2. What are the requirements that need to be fulfilled to establish cloud federations?

RQ1.3. What are the challenges that have been identified and required attention in the Cloud Federation Formation?

RQ1.4. What are the latest research trends in the exploration of applied theories, methodologies, criteria influencing Cloud Federation Formation, evaluation metrics, and experimental environments utilized to measure the proposed solutions?

The second objective of this study is to evaluate the impact of institutional trust on the cross-border cloud federation formation and address the issue of trust aggregation in the process. The formation of a

cross-border trusted cloud federation has the potential to address several challenges associated with cloud computing, including data security, privacy, and regulatory compliance. Institutional quality, which refers to the quality of the legal and regulatory framework within which cloud service providers operate, is a critical factor in ensuring the success and sustainability of a cross-border trusted cloud federation. This secondary objective aims to evaluate the effects of institutional trust on the overall trust evaluation process and decision-making for cloud federation formations. Additionally, it aims to address the issue of trust aggregation in cloud federation formation, given that feedback collected from users and/or peer providers may be subject to bias and exaggeration, including false feedback attacks. To achieve these secondary objectives, the study poses two research questions (RQs) that the study attempts to answer by proposing a trust evaluation model for game theory-based cloud federation formation.

RQ 2.1. How does incorporating institutional trust impact the overall trust evaluation process and consequently influence decision-making for cloud federation formations?

RQ 2.2. How do we ensure the accuracy of trust calibration in cloud federation formation when feedback collected from users and/or peer providers is subject to bias and exaggeration, including false feedback attacks?

1.4. Research Methodology

The research methodology used in this study consists of two distinct approaches for two separate studies. The research methodology adopted for the first study (Chapter Three) is a systematic literature review, which is a rigorous and transparent process of identifying, evaluating, and synthesizing the existing primary study on a specific topic or question. The study follows the systematic literature review proposed by Okoli (Okoli, 2015), which consists of several steps categorized into four stages: planning, selecting, extraction, and execution. The research question is defined in the planning stage, and the inclusion and exclusion criteria are determined at this stage. Then the next stage is selection, where the primary studies are identified by applying a search strategy. To do so, three databases are selected to collect the primary studies, namely, Scopus, web of Science, and science direct. Using several keywords combinations, the primary study is identified, and the relevant studies are selected based on the inclusion and exclusion criteria. Furthermore, the Kitchenham (Kitchenham et al., 2015) quality appraisal method is utilized to evaluate the quality of the selected studies. Once the study is identified, the next stage is data extraction to extract relevant information from the study to answer the research questions. Finally, in the execution stage, the result and outcome of the SLR are presented and discussed in a clear and structured

manner to answer the research question. The purpose of using this approach is to gain a comprehensive understanding of the cloud federation formation research area with enabling factors, requirements, challenges, and current threats.

The second study (Chapter Four) aims to examine the effect of institutional trust on the trust evaluation of cloud federation formation when there is not enough evidence to measure trust and there is uncertainty. Furthermore, it aims to address the issues faced by small providers regarding false-feedback attacks and bad-mouthing attacks. To conduct this study, an agent-based modeling approach, which is a computational approach that simulates the behavior and interactions of autonomous agents in a complex system, and a Python program, which is a popular and powerful language for data analysis and scientific computing, is used to develop the proposed algorithms and trust evaluation mode. The proposed trust evaluation model and algorithm are implemented and then the model verifying and validation are conducted. The experiments are conducted under different scenarios to validate the proposed approach's effectiveness.

1.5. Significance of the Study

As the demand for cloud computing grows, so does the number of cloud service providers and the variety of services they offer. However, according to (Mary, 2023, p. 10), the top 10 public service providers

control around 80% of the cloud market, leading to market concentration for the cloud market(Nazareth & Choi, 2021; Song, 2017) and vendor lock-in issues for consumers(Opara-Martins et al., 2016). Furthermore, small and medium-sized cloud service providers face challenges such as market inclusivity, resource inelasticity, and competition on price and performance (K. Kim et al., 2014). To address these issues, small providers cooperate with each other to create a larger cloud service by renting resources from each other. This business model is known as cloud federation. Small and medium cloud providers establish cloud federations for several reasons.

- To increase their reach and market share (Coronado & Altmann, 2017; Emeakaroha et al., 2017; Haile & Altmann, 2015)
- To expand their business opportunities (Abdo et al., 2015)
- To improve their reliability and availability(Coronado & Altmann, 2017)
- To reduce their costs(Kertesz, 2014)
- To improve their security and QoS(Haile & Altmann, 2015)
- To meet regulatory requirements(Haile & Altmann, 2015)
- To provide a more consistent user experience (Kertesz, 2014)
- To accelerate innovation, and so on.

However, cloud federation is not widely seen in the commercial market due to several reasons, including lack of standardization, lack of

trust between cloud service providers, interoperability issues, and lack of schemes for revenue sharing, coordinated resource management, and resource provisioning. One way to address these challenges is through the development of standards for cloud federation. In collaboration with IEEE, the National Institute of Standards and Technology (NIST) has been working on the development of a reference architecture for cloud federation. This joint effort has led to the release of the IEEE 2302-2021 standard, which focuses on achieving intercloud interoperability and Federation (SIIF)(Bohn & Lee, 2022).

In addition, several studies explore the issue of the lack of cloud federation's wide commercialization from different perspectives. These studies explore several aspect of cloud federation realization; some are presented in Table 1.2.

Table 1. 2. Related studies to addressing the challenges of cloud federation in practice

The studies perspective to addressing the challenges of cloud federation practices	**Studies**
Cloud federation Business model	(Yang et al., 2012)
Incentivizing cloud providers to establish/join cloud federation	(Aryal, 2019; Coronado & Altmann, 2017)
Economic model for revenue sharing	(Aryal & Altmann, 2017; Darzanos

between cloud federation members	et al., 2015, 2019, 2016, p. 41; Í. Goiri et al., 2012; Samaan, 2014)
Cloud resources Migration strategy	(Addya et al., 2019; Cerroni, 2015; Sun et al., 2016)
Resource discovery and Matchmaking	(S. Latif et al., 2022; Messina et al., 2014; Rebai, 2017; Toosi et al., 2011)
Workload management	(K. Li, 2022; Sajid et al., 2021)
Architectural Strategy	(Altmann et al., 2016; Assis & Bittencourt, 2016; Bohn et al., 2020)
Market Strategy	(Ramezani et al., 2022)

Although several studies address the issue of cloud federation practices from a different perspective, as of our knowledge, no study addresses the market competition issue especially faced by small and medium cloud service providers. Therefore, this research aims to improve market competition for small and medium cloud service providers by providing the reference guideline for cloud providers to make informed decisions on when to establish/join a cloud federation, what are the driving factors towards it, what requirements need to be fulfilled and what challenges they might face during the process. Although there are alternative ways to enhance competition in the market,

such as individual efforts by cloud service providers or specialization, this research focuses on cloud federation formation as a merger and acquisition or joint venture strategy to empower small and medium cloud service providers to establish cloud federation. It is possible for SMEs to compete more effectively with larger players by forming strategic alliances and leveraging shared resources(Dodourova, 2009; Elmuti & Kathawala, 2001; Mowla, 2012; Russo & Cesarani, 2017; Yasuda, 2005).

This research also considers the application of strategic alliance theory to analyze the dynamics of these collaborations and provide valuable insights into the decision-making processes of cloud service providers. Furthermore, the research also focused on tackling the challenge of trust evaluation in partner selection strategies for cloud federation formation, specifically aiming to address the concerns of small and medium cloud service providers. Thus, the research aims to contribute to improving market competition by providing a strategy for fair, inclusive, and unbiased trust evaluation for enabling small and medium cloud service providers to compete on a more equal footing, benefiting customers and fostering innovation within the cloud computing industry.

1.6. Research Contribution

This research aims to contribute to the existing field of cloud federation by exploring the enabling factors, requirements, and challenges of cloud federation formation and providing a novel architecture, algorithm, and trust evaluation model to ensure the trusted cloud federation formation. Two studies with detailed analysis using different approaches are offered on cloud federation formation.

The first study involved the detailed analysis of 63 studies in cloud federation formation and provides a comprehensive analysis of proactive and reactive enabling factors that cloud managers need to consider when deciding to form a cloud federation. The study also examines the requirements for forming a cloud federation and the challenges that may arise during the process. By providing this information, the study helps cloud managers make informed decisions about when to establish a cloud federation and how to overcome possible challenges. Furthermore, the study provides insights into the current trends in cloud federation formation and helps understand the dynamics of cloud federation in relation to the existing literature. The followings are key contributions from the first study.

- Provides inputs that can be used to develop standardization frameworks for cloud federation formation. The frameworks can be used to guide cloud service providers on the necessary steps

required to form federations, including the enabling factors and the requirements.

- Provide a theoretical framework utilizing strategic alliance formation theories to analyze enabling factors for cloud federation and identify any gaps, ultimately providing insight into the complexity of technology strategic alliances
- Highlight the importance of trust in the establishment and maintenance of cloud federations and emphasize the need for consideration of formal institutions, such as laws and regulations, in addition to informal institutions, to effectively establish cross-border collaborations.
- Provides an overview of the various methodologies used to address the challenge of cloud federation stability. Specifically, the study found that a majority of the studies addressed the issue of stable coalition formation through mathematical proof, with a focus on Nash stability and individual stability.
- Highlights the prevalence of game theory in establishing cloud federations, and how it can be used to analyze players' opportunistic behavior and predict outcomes in real-world scenarios.

The second part of the study proposes a novel trust evaluation model that highlights the importance of incorporating external

(institutional) trust indicators along with internal (organizational) trust sources to compute fair, inclusive, and multidimensional trust assessment. The model includes institutional trust indicators and peer recommendations as a factor to assess trust when not enough information is available to compute trust. The study also demonstrates that the certainty of the cloud service provider trust impacts the role of institutional trust in selecting potential partners for cloud federation formation. The study further provides a continuous trust aggregation approach to evaluate trust utilizing direct and indirect (computed from peer cloud providers' feedback and user feedback) trust factors. For indirect trust, the confidence score evaluation is provided to feedback from peer providers and users. Where a confidence score is used to ensure accurate decision-making. This approach has been shown to effectively identify malicious feedback in trust evaluations and reduce the chances of false positives and false negative feedback. The followings are key contributions from the second study.

- Modeling and proposing the distributed trust evaluation that considers the internal and external trust sources.
- Proposed trust aggregation approaches utilizing direct and indirect trust sources along with the indirect source confidence score measure.

- Highlights the role of institutional trust in improving the certainty of subjective trust evaluations in Cloud Federation Formation.
- Highlight the importance of incorporating confidence score in the feedback-based trust evaluation model.

1.6. Research Outline and Design

The research comprises five chapters that provide a comprehensive overview of the study. Chapter 2 provides the background and literature review of cloud federation formation, including the relevant history and lifecycle of cloud federation. Chapter 3 presents a systematic literature review of cloud federation formation. This focuses on the foundations of cloud federation formation enabling factors, requirements, challenges, and current trends in the field. Chapter 4 describes institutional quality-aware cloud federation formation and employs a simulation experiment approach to address trust issues faced by small providers. Finally, Chapter 5 provides a summary of the main findings, contributions, limitations, and suggestions for future research. The research outline provides a clear roadmap for the study, helping readers understand the research process and objectives.

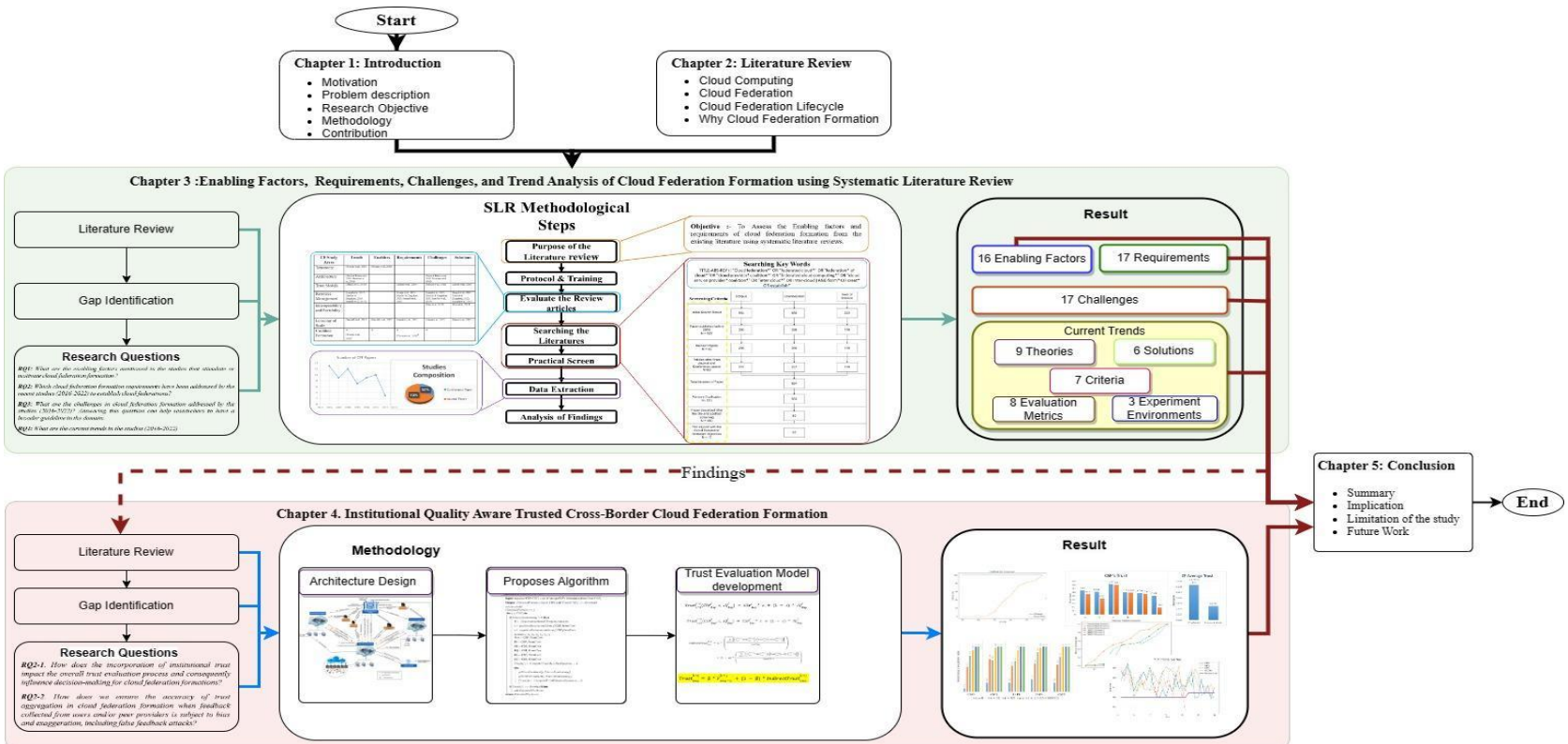


Figure 1. 1. Research framework

Chapter 2. Literature review

2.1. Cloud Computing

Cloud computing is the method of providing computing services, such as servers, storage, databases, networking, software, analytics, and intelligence, over the Internet (Bisong, 2019). It involves the strategy of storing, overseeing, and processing data using a network of distant servers hosted on the Internet, rather than utilizing a local server or an individual's personal computer (Bisong, 2019; Hayes, 2008). It provides numerous advantages, including cost savings, speed, scalability, productivity, performance, dependability, and security. Cloud computing allows users to access and use these services on demand without owning or managing the physical infrastructure (Arutyunov, 2012).

Cloud computing has a long history, stretching back to the 1950s, when users could share large-scale mainframes through the use of terminals and share them with other users (Evwiekpaefe & Ajakaiye, 2013). As a result of IBM's introduction of virtualization technology in the 1970s (Bell, 1985), various operating systems were able to run simultaneously on a single physical machine. Since the 1990s, users have been able to access data and software from anywhere in the world thanks to the internet and web-based application (Qiu & Gooi, 2000). Over the years, Compaq Computer Corporation has been the first company to

come up with the term "cloud computing"(Antonio, 2011; Jones et al., 2019). During the 2000s, cloud computing emerged as a new paradigm, offering individuals and organizations flexible, scalable, and cost-effective services through the use of the Internet. Amazon Web Service (AWS) was the first tech company to introduce its cloud-based services at that time, followed by other tech companies like Google and Microsoft shortly after (Patel, 2018).

Some of the milestones in the history of cloud computing are:

- In 1961, John McCarthy of MIT envisioned the idea of cloud computing as a computer utility, envisioning a future where computers similar to the ones he advocated for could be utilized as a public utility, much like the telephone system (Xu et al., 2023).
- In 1999, Salesforce.com made its debut as one of the pioneering cloud-based software-as-a-service (SaaS) providers, delivering customer relationship management (CRM) applications via the internet (Bielawski et al., 2015).
- In 2002, AWS introduced its web-based retail services platform, which later evolved into a suite of cloud services such as computing, storage, database, and networking.
- In 2006, AWS launched its Elastic Compute Cloud (EC2) and Simple Storage Service (S3), which allowed users to rent virtual

machines and store data in the cloud (Patel, 2018; Zhang et al., 2010).

- In 2008, Google introduced its App Engine platform, providing developers with the capability to create and host web applications using Google's infrastructure (Roche & Douglas, 2009).
- In 2010, Microsoft introduced its Azure platform, providing a comprehensive array of cloud services encompassing computing, storage, databases, analytics, and machine learning capabilities (Zhang et al., 2010).
- In 2011, IBM launched its SmartCloud portfolio, which included cloud-based solutions for enterprise IT and business processes (IBM, 2011).
- In 2012, Dropbox announced that it had reached 100 million users for its cloud-based file hosting service (Constine, 2012).
- In 2016, Netflix announced that it had completed its migration to AWS, becoming one of the largest cloud customers in the world.(BRODKIN, 2016)
- In 2019, Google acquired Looker, a cloud-based business intelligence platform (Richardson et al., 2020).

2.2. Cloud Federation

Cloud federation is an approach to addressing the challenges of cloud computing, such as interoperability (Kurze et al., 2011)and

flexibility(Lee, 2016), by extending the capabilities of cloud computing. This concept has been defined in various ways by multiple sources in the literature and reports. According to NIST (Bohn et al., 2020), cloud federation is defined as a process of combining resources from a variety of cloud providers into a common pool of resources that consumers can access based on their needs and preferences through a single point of access. It is a term that refers to the collaboration and cooperation among different cloud providers to share and exchange resources and services across their domains (Kertesz, 2014). Cloud federation can enable cloud providers to offer more diverse and flexible services to their customers, as well as to optimize their resource utilization and costs. Cloud federation can also benefit cloud customers by providing them with more choices, better performance, higher availability, and lower prices (Kurze et al., 2011; Phani Krishna Kollapur Gandla, 2023; T, 2020).

Cloud federation has its roots in the history of cloud computing, which can be traced back to the 1950s (Evwiekpaefe & Ajakaiye, 2013) when large-scale mainframes were shared by multiple users through terminals. The concept of cloud federation is not attributed to a single person or organization but rather evolved from the idea of cloud computing over time. Some of the early contributions to cloud federation include J.C.R. Licklider, who envisioned an “intergalactic computer network” in the 1960s that would allow users to access data and

programs from anywhere (Licklider, 1963), IBM, who introduced virtualization technology for mainframes in the 1970s that enabled multiple virtual machines to run on a single physical node(Obasuyi & Sari, 2015), NASA, who developed Nebula, open-source software emerged to facilitate the deployment of private and hybrid clouds and enable cloud federation (Kollolu, 2020; Loubière & Tomassetti, 2020), and the RESERVOIR project, a European Commission-funded project that enhanced Nebula and demonstrated cloud federation across multiple providers and countries in 2009(Muthu, 2016; Rochwerger et al., 2009).

The idea of cloud federation was first proposed by (Buyya et al., 2009), who envisioned a "market-oriented" cloud architecture allowing cloud providers to dynamically trade resources and services based on supply and demand(Buyya et al., 2009). They defined cloud federation as "the union of several smaller clouds that aim at sharing resources in order to gain benefits such as scalability, resilience, and geographic distribution." They also proposed a federated cloud resource broker that would act as an intermediary between cloud providers and customers, facilitating the discovery, negotiation, allocation, and execution of cloud services (Buyya et al., 2009).

Since then, many researchers have explored different aspects and challenges of cloud federation, such as:

- Definition and taxonomy: Several studies have attempted to provide a clear and comprehensive definition and classification of cloud federation, based on different criteria and perspectives (Abdo et al., 2014; Bohn et al., 2020; Grozev & Buyya, 2014; Kurze et al., 2011; Lee, 2016; Toosi et al., 2014). For example, Celesti et al. (2010) proposed a taxonomy of cloud federation based on the level of integration (horizontal or vertical), the type of relationship (peer-to-peer or hierarchical), the degree of autonomy (independent or dependent), and the scope of the federation (intra-cloud or inter-cloud). Grozev and Buyya (2014) proposed a taxonomy of cloud federation based on the nature of collaboration (cooperative or competitive), the type of service (infrastructure-as-a-service or platform-as-a-service), the mode of operation (static or dynamic), and the objective of the federation (performance or cost).
- Architecture and design: Several studies have proposed various architectures and designs for cloud federation(Assis & Bittencourt, 2016; Bohn et al., 2020; Grozev & Buyya, 2014; Kertesz, 2014, 2014; Rochwerger et al., 2009), addressing different requirements and scenarios(Ahmed et al., 2019a; Kousiouris et al., 2013; Lee, 2016; Panarello et al., 2014). For example, Celesti et al. (2010) proposed a reference architecture

for federated cloud computing that consisted of four layers: infrastructure layer, virtualization layer, coordination layer, and service layer. They also defined a set of functional components for each layer, such as resource manager, virtual machine manager, federation manager, service manager, etc.

2.3. Cloud Federation Lifecycle

The cloud federation lifecycle hasn't been clearly stated in the previous study except expressed in the standard documents (Bohn et al., 2020). However, to understand the foundation of the cloud federation lifecycle, we adopt the strategic alliance lifecycle in any international business and allied to the cloud federation perspective since cloud federation is the strategic alliance between cloud service providers (Haile & Altmann, 2015). According to Russo & Cesarani, (2017), the strategic alliance lifecycle consists of three phases: formation phase, operation phase, and termination phase. On the other hand, Piroozi et al., (2021) summarize the strategic alliance lifecycle into three, alliance formation, alliance operation, and alliance evaluation phase. Similarly, cloud federations have the Formation(Alam et al., 2020; Dinachali et al., 2022a; Mashayekhy et al., 2021), Operation, Evaluation, and Termination phases. is a term that refers to the process of establishing, maintaining, and terminating a federation relationship between two or more cloud

providers. The cloud federation lifecycle typically involves the following stages:

2.3.1. Formation Phase

The first cloud federation phase is the formation phase, where potential cloud service providers are identified, assessed, negotiated, and formalized (Alam et al., 2020; Dinachali et al., 2022a; Mashayekhy et al., 2021). At this stage, the cloud service providers should establish the strategic rationale, common objectives value proposition, roles and responsibilities of each partner, governance, and legal aspects of the alliance. In this stage, the main activities are resource discovery, negotiation, and establishment.

- **Discovery**: This is the process where cloud providers discover each other and exchange information about their capabilities(Govil et al., 2012; Khandelwal et al., 2016; Tricomi et al., 2020), policies(Kousiouris et al., 2013), and requirements for federation(Messina et al., 2014). This can be done through manual or automated methods, such as using a broker service or a registry service.
- **Negotiation**: This is the process where cloud providers negotiate the terms and conditions of the federation agreement, such as the scope, duration, service level agreements (SLAs)(Ghenai & Nouioua, 2020; Messina et al., 2016; Petri, Zou, et al., 2015),

pricing(Das, 2015; K. Li, 2021), security(Bernsmed et al., 2011), trust(Gupta & Annappa, 2016), and governance(Comi & Fotia, 2018; Messina et al., 2017). This can be done through contracts or protocols, such as using a trust framework or a standard specification.

- **Establishment**: This is the process where cloud providers establish the technical and operational mechanisms for enabling federation, such as configuring the identity and access management systems(Dhanabagyam & Karpagam, 2018; Samlinson & Usha, 2013; Thomas & Sekaran, 2014), setting up the network connections(Abusitta et al., 2018a; Bairagi et al., 2016), provisioning the resources(Halabi et al., 2018; Hassan et al., 2014a; Toosi et al., 2011), and monitoring the performance(Al Falasi et al., 2013; Aversa & Tasquier, 2018; Ramezani et al., 2022). This can be done through APIs or tools, such as using a federation manager or an orchestration service (Abdo et al., 2013; Gebrealif et al., 2020, 2021).

2.3.2. Operation and Management Phase

The second phase of the strategic alliance between cloud service providers (cloud federation) is operation and management phase, where cloud providers operate and manage the federated services and resources according to the federation agreement, such as resource placement and

allocation (Casalicchio & Silvestri, 2012; Larsson et al., 2011; Messina et al., 2014; Shan et al., 2012), delivering the expected quality of service (QoS), governance (Andrea et al., 2017), resolving issues, billing customers (Elmroth et al., 2009), and auditing activities (Alansari et al., 2017; Anastasi et al., 2014). Moreover, the cloud provider can make a decision to outsource resources within or outside the federation (I. Goiri et al., 2010). The cloud providers should align their operational plans and processes with the terms and scope of the alliance, measure and communicate their performance and progress (Anas et al., 2017; Hassan et al., 2011, 2012, 2014b), manage their relationships and risks, and collaborate and learn from each other. They should also ensure that the trust, security, resource sharing, and usage issues are addressed and resolved in the cloud federation.

2.3.3. Evaluation Phase

The third cloud federation phase is evaluation, where the cloud providers review and analyze their alliance results and feedback, and identify the strengths and weaknesses of the alliance. Cloud providers should improve their effectiveness and efficiency(Darzanos et al., 2015; Duan, 2017; Giacobbe et al., 2015; Haile & Altmann, 2018; Kanwal et al., 2014), renew and redefine their trust and commitment(Ahmed et al., 2019a; Bernabe et al., 2015; Kanwal et al., 2014), and adapt to changing

conditions and expectations. They should also consider the possibility of transforming or dissolving the alliance if necessary.

2.3.4. Termination Phase

The fourth cloud federation phase is termination, where the cloud providers leave the cloud federation. It is the stage where cloud providers terminate the federation relationship when it is no longer needed or desired(Gorjian Mehlabani & Zhang, 2023; L. Li et al., 2022) such as due to agreement expiration(Zant et al., 2013), SLA violation(Hussain et al., 2016; Nawaz et al., 2019), dissatisfaction(Abdo et al., 2015), or change of circumstances. This can be done through notifications or actions, such as using a termination protocol or a provisioning service (Mashayekhy & Grosu, 2013).

2.4. Why Cloud Federation Formation

According to Mowla, (2012), Although a new alliance appears to be formed nearly every 90 seconds, it appears that nearly 60 percent of the alliances formed are likely to fail(Elmuti & Kathawala, 2001; Mowla, 2012). This is due to the fact that although the alliance is a popular strategy, they are not always successful. The alliance formation stage is critical because it sets the foundation and direction of the alliance, as well as establishes trust and commitment among the partners (Bucklin & Sengupta, 1993). A poorly formed alliance may lead to misalignment, conflict, and failure in the later stages (Dodourova, 2009; Zamir et al.,

2014). Therefore, it requires careful planning and management to achieve the intended benefit (Bucklin & Sengupta, 1993).

Similarly in cloud federation, cloud federation formation is a critical stage to discover, select, and negotiate with the appropriate cloud providers to partner with given several criteria and metrics (Alam et al., 2020; Das et al., 2014; Dhole et al., 2016; Dinachali et al., 2022a; Mashayekhy et al., 2021). In this stage, the requirements and expectations of each participating cloud service provider, the governance framework, and the operational procedures that will govern the federation need to be defined. During this phase, the participating cloud service providers collaborate to develop a shared vision and strategy for the federation. They identify the services they will offer, and agree on the federation's terms and conditions.

The cloud federation formation phase is critical because it sets the foundation for the entire federation, and any issues or shortcomings during this phase can have significant impacts on the success of the federation. During this phase, the participating cloud service providers collaborate to establish a shared vision and strategy for the federation, identify the services they will offer, and agree on the terms and conditions of the federation.

Here are some reasons why the cloud federation formation phase is so important:

- Ensuring Compatibility: The participating cloud service providers need to ensure that they are interoperable in terms of technology, architecture, and business models (Emeakaroha et al., 2017; Jamba & Aluvalu, 2016). This compatibility is essential to ensure that the federation operates seamlessly and delivers high-quality services to its customers (Dhole et al., 2016; Mashayekhy et al., 2021).
- Establishing Governance: The formation phase is crucial for establishing the governance framework of the federation, which ensures that the federation operates in a transparent and accountable manner (R. Latif et al., 2021; Lee, 2016). The governance framework should include policies, procedures, and mechanisms to resolve disputes and conflicts among the participating cloud service providers.
- Building Trust: Trust is a crucial factor in the success of a cloud federation. During the formation phase, the participating cloud service providers must establish trust among themselves by sharing information, resources, and expertise (Abawajy, 2011; Ahmed et al., 2019b; Gupta & Annappa, 2016; Kanwal et al., 2014; Mashayekhy et al., 2021). This trust-building effort is essential to foster collaboration and ensure the long-term success of the federation.

- Ensuring Scalability: The formation phase must also consider the scalability of the federation (S. Latif et al., 2022). The participating cloud service providers should be able to expand or contract their services as per the changing needs of the customers. This ensures that the federation remains relevant and competitive in the long run.
- Establishing Business Relationships: The formation phase is an opportunity for the participating cloud service providers to establish business relationships with each other. These relationships are crucial to the success of the federation and can lead to new opportunities for the cloud service providers to expand their businesses.

2.5. Cloud Federation in Practical Perspectives

In various industries like finance, healthcare, education, telecommunications, research, academia, and energy, small and medium-sized enterprises implement federation strategies to enhance market competition (Gemser et al., 2012; Kamalian et al., 2015, 2015; Mohamad, 2012). In the automotive industry, the Renault-Nissan-Mitsubishi Alliance showcases the power of collaboration (Segrestin, 2005; STEVENS, 2008), while the Oneworld Alliance in the airline industry enables seamless travel experiences for customers (Göv, 2020). The Airbus Consortium brings together European aerospace companies

to collaborate on aircraft design and production (Petrescu et al., 2017). Similarly, the Star Alliance connects major airlines to enhance passenger connectivity (Czipura & Jolly, 2007), and Semiconductor manufacturing companies in China form the SMIC alliance to compete globally (Yu et al., 2017).

Table 2. 1. The difference and commonalities of Cloud federation with Federation in other sectors

Feature	**Cloud Computing**	**Other sectors**
Managed by	Third-party provider or the cloud providers itself	Organization itself
Purpose	To share data, knowledge, and resources	To improve collaboration and efficiency
Benefits	Improved collaboration, efficiency, cost savings	Improved collaboration, efficiency, cost savings
Complexity	High	Medium
Cost	Can be expensive to set up and maintain	Can be less expensive to set up and maintain but still requires some investment
Formation type	Dynamic and Static federation	Static Federation

Federation in cloud computing shares many similarities with the federation in other sectors. The main goal of a federation is to connect multiple resources to create a unified environment while still allowing individual entities to retain their autonomy. This enables scalability, performance improvement, and cost reduction. However, there are also challenges related to trust between the participants and security concerns such as privacy leakage. These challenges are common across different sectors that implement federation. The uniqueness of cloud federation lies in its novelty, and emerging technology. Cloud federation focuses on connecting multiple cloud computing services to create a scalable and cost-effective computing platform. This involves challenges such as ensuring data privacy and security, managing resource allocation, and maintaining service-level agreements. However, its potential benefits are substantial, leading to its growing popularity. Despite being a relatively new and evolving technology, cloud federation shows great promise in various sectors. Organizations are actively exploring and implementing initiatives and practices of cloud federation to leverage its potential benefits. The followings are the cloud federation practices.

2.5.1. ARISTOTLE Cloud Federation

The ARISTOTLE Cloud Federation is an initiative supported by the U.S. National Science Foundation (NSF) aimed at creating a federated cloud infrastructure to assist scientists and engineers in

performing elastic workflows and analyzing large-scale datasets (Vaillancourt et al., 2021). This project seeks to develop a collaborative model for sharing data analysis resources among institutions, commercial clouds, and NSF cloud resources, promoting flexibility, resource sharing, and fair resource access across multiple institutions while serving as a blueprint for campus cyber infrastructure (Knepper et al., 2019; Vaillancourt et al., 2021).

2.5.2. BEACON (Enabling Federated Cloud Networking)

The BEACON project is a collaborative research initiative aimed at developing and implementing a scalable and secure federated cloud infrastructure (Moreno-Vozmediano, et al., 2016). The project's primary goal is to enable seamless interconnection and collaboration between multiple independent cloud infrastructures while ensuring data privacy, security, and efficient resource utilization (Massonet & Sheridan, 2016; Moreno-Vozmediano, et al., 2016). The project aims to address challenges related to cloud federation and provide practical solutions to foster interoperability and trust among federated clouds.

2.5.3. Data Federations (Cloud federation use case)

Data federation refers to the concept of integrating and accessing distributed data sources as a unified view, regardless of their physical location or storage systems (Gardner et al., 2014; *U.S. Data Federation*, n.d.). It involves combining data from multiple sources into a coherent

and virtualized representation, enabling efficient data access and analysis. In the context of cloud federation, data federation becomes essential for facilitating seamless data sharing and integration across multiple federated clouds (Gu et al., 2022). By federating data, organizations can leverage the strengths of different cloud providers or independent cloud infrastructures within a federation, enabling collaborative data analysis, improved data availability, and more comprehensive insights across distributed environments. Data federation is a critical component of cloud federation, ensuring that data can be securely accessed and utilized across federated clouds to support complex applications and data-driven decision-making(Carlini et al., 2021). Some examples of data federation practices are:

- ***U.S. Data Federation***: It is an initiative aimed at enhancing distributed data management capabilities, addressing challenges related to data interoperability, and promoting the development of broader data standards across the government (Lindpaintner, 2019; *U.S. Data Federation*, n.d.).
- ***Global Alliance for Genomics and Health (GA4GH)***: initiative, which focuses on federating genomic data from multiple research institutions worldwide (Birney et al., 2017; Rahimzadeh et al., 2016). Through the development of interoperability standards and data-sharing frameworks, GA4GH enables researchers to

access and analyze genomic data across federated clouds, promoting collaboration and accelerating genomics research (Birney et al., 2017; Kathryn North, 2015; Terry, 2014).

- ***Atlas Data Federation***: A service within MongoDB that amalgamates information from your MongoDB Atlas clusters, Atlas Data Lake, and cloud storage to create virtual databases and collections. (*Atlas Data Federation Overview — MongoDB Atlas*, n.d.; Berghaus et al., 2019; Gardner et al., 2014).

2.5.4. Federated Learning (Cloud Federation use case)

Federated learning represents a machine learning strategy allowing model training across numerous decentralized devices, eliminating the necessity of transmitting raw data to a central server (L. Li et al., 2020). Federated learning and cloud federation combine to enable collaborative and privacy-preserving machine learning across distributed environments (L. Liu et al., 2019, 2020). Federated learning allows training models on decentralized devices while preserving data privacy, and cloud federation provides the necessary infrastructure and resources for efficient management and orchestration of the federated learning process (T. Liu et al., 2021; Stergiou et al., 2022). By leveraging cloud federation, organizations can scale the federated learning process, process large datasets, and improve performance. Together, federated learning with cloud federation enables scalable and privacy-conscious

machine learning across multiple cloud infrastructures. Some examples of federated learning practices are:

- ***TensorFlow Federated***: Developed by Google, TensorFlow Federated is an open-source framework that allows distributed machine learning on decentralized data sources (Bonawitz et al., 2019). It provides the necessary tools and APIs for implementing federated learning algorithms (Kholod et al., 2021).
- ***PySyft***: PySyft is a Python library for federated learning and privacy-preserving machine learning. It integrates with popular deep learning frameworks like PyTorch and TensorFlow and provides functionality for secure and privacy-conscious model training (Kholod et al., 2021).
- ***NVIDIA Clara Federated Learning***: NVIDIA Clara is a healthcare-focused platform that includes federated learning capabilities (Abreha et al., 2022; Kholod et al., 2021; Ng et al., 2021). It enables collaboration and model training across multiple healthcare institutions while ensuring data privacy and compliance (Kholod et al., 2021).
- ***IBM Federated Learning***: IBM offers a federated learning framework that allows organizations to train machine learning models using distributed data while preserving data privacy (Abreha et al., 2022; Joshi et al., 2022). It provides tools and

infrastructure for managing and orchestrating the federated learning process (Kholod et al., 2021).

2.6. Cloud Federation in Policy Perspective

The Cloud Federation Policy perspective encompasses the policies and regulations that govern the implementation and operation of cloud federation (Darzanos et al., 2016; Kertesz & Varadi, 2014). These policies aim to address various aspects such as data privacy(Kertesz & Varadi, 2014), security(Massonet, Levin, et al., 2016), compliance (Massonet et al., 2011), and interoperability(Bavier et al., 2012; Bohn et al., 2022; López García et al., 2016; Sitaram et al., 2016). Here are some of the key elements of the Cloud Federation Policy perspective:

2.6.1. Data Privacy and Protection

Many countries and regions have enacted data protection laws, such as the GDPR in the European Union (Voigt & von dem Bussche, 2017) or the California Consumer Privacy Act (CCPA) in the United States (Bukaty, 2019). These regulations define the privileges individuals possess over their personal data and place responsibilities on entities that manage and process such data. Cloud federation policies need to ensure that data transferred or shared across federated clouds is adequately protected and that users maintain control over their data (Alansari et al., 2017; Mashayekhy et al., 2014; Rahimzadeh et al., 2016). Policies may include requirements for data encryption, access controls,

data breach notifications, and data residency restrictions (Kousiouris et al., 2013; Lee, 2016; Mashayekhy et al., 2014).

2.6.2. Security and Compliance

Cloud federation policies address the security aspects of federated cloud environments (Massonet, Levin, et al., 2016; Massonet et al., 2011; Zant et al., 2013). The cloud federation security outline guidelines for implementing robust security measures to protect against unauthorized access, data breaches, and other security risks (Bernsmed et al., 2012; Massonet, Levin, et al., 2016). Compliance with industry standards, certifications, and regulatory requirements is also emphasized (Barreto et al., 2015a). Policies may require regular security audits, vulnerability assessments, incident response plans, and adherence to specific security frameworks like ISO/IEC 27001, ISO/IEC 27032, and ISO/IEC 27017(Tissir et al., 2021).

2.6.3. Interoperability and Standards

Cloud federation policies emphasize the need for interoperability and standardization to enable seamless communication and integration between different cloud platforms within a federated environment (Bohn et al., 2020, 2022; Lee, 2016; Thakur & Shrivastava, 2015). It may promote the adoption of common APIs, data formats, and protocols to facilitate data and workload portability (Bohn et al., 2022; López García et al., 2016). Standardization bodies such as ISO and NIST play a crucial

role in developing and maintaining standards for cloud federation (Bohn et al., 2020; Bohn & Lee, 2022).

2.6.4. Governance and Accountability

Cloud federation policies and standards establish guidelines for governance and accountability in cloud federation (Bohn et al., 2020; Bohn & Lee, 2022). It define the roles and responsibilities of cloud service providers, customers, and other stakeholders (Bohn et al., 2020). Policies may require transparent reporting, audit trails, and mechanisms for dispute resolution. It also address issues related to liability, indemnification, and service-level agreements between participating entities.

2.6.5. Cross-Border Data Transfer

Cloud federation policies may address the challenges associated with cross-border data transfers (Kousiouris et al., 2013; Sullivan, 2014). It ensures compliance with international data transfer regulations and considers factors such as data sovereignty, jurisdictional issues, and local data protection law (Celesti et al., 2012; Mashayekhy et al., 2014). Policies are required for providers to implement appropriate safeguards, such as binding corporate rules (BCRs) or standard contractual clauses (SCCs), to facilitate lawful and secure data transfers(Emeakaroha et al., 2017; Kertesz & Varadi, 2014; Massonet, Dupont, et al., 2016; Massonet et al., 2011).

Therefore, in general, the cloud federation policy perspective seeks to create a regulatory framework that promotes the secure, compliant, and interoperable operation of federated cloud environments(Bernsmed et al., 2011; Bohn & Lee, 2022; Kertesz & Varadi, 2014; Mashayekhy et al., 2014; Massonet, Dupont, et al., 2016; Thakur & Shrivastava, 2015; Voigt & von dem Bussche, 2017). These policies aim to protect user data, ensure accountability, and foster trust among participants in the cloud federation ecosystem.

2.7. Cloud Federation in Theoretical Perspective

The Cloud Federation Theoretical perspective focuses on the conceptual and theoretical frameworks that underpin the concept of cloud federation (Assis et al., 2014a; Barreto et al., 2015b). It involves understanding the fundamental principles, models, and theories that guide the design, architecture, and operation of federated cloud environments(Abusitta et al., 2018a; Al Falasi et al., 2016; Aryal, 2019; Assis et al., 2014b; Cayirci, 2013; Darzanos et al., 2016, 2016; Rochwerger et al., 2009). Some of the key elements of the Cloud Federation Theoretical perspective is explain as follow:

2.7.1. Distributed System and Virtualization

Theoretical foundations of cloud federation draw upon concepts from distributed systems and virtualization (Castañeda et al., 2019; Gebrealif et al., 2020, 2021; D. Kim et al., 2019). Distributed systems

theory provides insights into how resources can be shared(Chen et al., 2017; Hassan et al., 2015; Wu et al., 2022), coordinated(Petri et al., 2017; Petri, Rana, et al., 2015), and managed across multiple cloud providers in a federated environment(Aazam & Huh, 2014; Carvalho et al., 2018; Khorasani et al., 2020; Ramezani et al., 2022). Virtualization enables the abstraction and isolation of resources, allowing efficient utilization and dynamic provisioning across federated clouds.

2.7.2. Resource Management and Allocation

Theoretical perspectives in cloud federation focus on optimizing resource management and allocation across participating cloud providers. This involves developing algorithms, models, and policies to dynamically allocate workloads, balance resource utilization, and optimize performance in a federated environment (Anas et al., 2017; Chen et al., 2017; K. Li, 2022). Resource management theories may consider factors such as workload characteristics, user requirements (Samlinson & Usha, 2013), cost efficiency (Altmann & Kashef, 2014; Dinachali et al., 2022a), and quality of service (QoS) guarantees (Ahmed, Al-Saidi, et al., 2021; Aliyu et al., 2017).

2.7.3. Interoperability and Standardization

Theoretical perspectives emphasize the importance of interoperability and standardization in a cloud federation (Jamba & Aluvalu, 2016; Thakur & Shrivastava, 2015). Theoretical frameworks

explore approaches for enabling seamless communication, data portability, and service integration between diverse cloud platforms. Standardization efforts, such as defining standard APIs, data formats, and protocols, are essential for achieving interoperability and ensuring efficient collaboration among federated clouds (Bohn et al., 2022; López García et al., 2016).

2.7.4. Trust, Security, and Privacy

Theoretical perspectives also address the trust(Abusitta et al., 2018b; Gupta & Annappa, 2016; Kanwal et al., 2014; Mashayekhy et al., 2021), security(Barreto et al., 2015a; Halabi & Bellaiche, 2020; Massonet, Levin, et al., 2016; Zant et al., 2013), and privacy(Feng et al., 2020; T. Liu et al., 2021) concerns associated with cloud federation. Theoretical frameworks may explore cryptographic techniques, access control models, authentication mechanisms, and privacy-preserving protocols to establish secure and trusted interactions between federated clouds. Theoretical approaches consider privacy-enhancing technologies, such as anonymization and differential privacy, to protect sensitive data in a federated environment.

2.7.5. Economic and Business Models

Theoretical perspectives delve into economic and business models related to cloud federation. They investigate cost models(Altmann & Aryal, 2020; Altmann & Kashef, 2014; Entrialgo et

al., 2021), pricing mechanisms(Dinachali et al., 2022b; Khandelwal et al., 2021; Y. Li et al., 2022), revenue-sharing models(Aryal & Altmann, 2017; Hassan et al., 2015), and incentive structures for incentivizing participation and collaboration among cloud providers(Aryal, 2019; Coronado & Altmann, 2017). Theoretical frameworks explore concepts like federated marketplaces, auction mechanisms, and game theory to optimize resource allocation and promote fair competition in a federated ecosystem.

2.7.6. Performance Evaluation and Optimization

Theoretical perspectives in cloud federation involve performance evaluation and optimization studies. They develop analytical models, simulation frameworks, and optimization algorithms to assess and improve the performance, scalability, and efficiency of federated cloud environments (Biran et al., 2017; Cao & Wu, 2018; Dhole et al., 2016; Veloso et al., 2016). Theoretical approaches may explore queuing theory, stochastic models, and optimization techniques to study system behavior, resource provisioning strategies, and workload scheduling algorithms(Casalicchio & Silvestri, 2012; Chen et al., 2017; Larsson et al., 2011; Su et al., 2020; Tricomi et al., 2020; Wu et al., 2022).

The Cloud Federation Theoretical perspective provides a foundation for understanding the underlying principle that defines the standard design and operation of federated cloud environments. By

exploring these theoretical frameworks, researchers and practitioners can develop novel approaches, algorithms, and architectures to address the challenges and optimize the performance of cloud federation.

Table 2. 2. Comparison table for Theoretical, Policy and Practical perspective of cloud federation

Criteria	**Theoretical Perspectives**	**Policy Perspectives**	**Practical perspectives**
Focus	Conceptual and theoretical frameworks	Policies and regulations	Real-world implementation and challenges
Key Elements	• Distributed systems and virtualization • Resource management and allocation • Interoperability and standardization • Trust, security, and privacy • Economic and business	• Data privacy and protection • Security and compliance • Interoperability and standards • Governance and accountability • Cross-border data transfers	• Interoperability • Security concerns • Resource allocation • Practical challenges

	models • Performance evaluation and optimization		
Evaluation	Analytical models, simulation frameworks, optimization algorithm	Compliance with legal frameworks, adherence to data protection laws, adherence to security frameworks	Identification and analysis of practical challenges evaluation and implementation
Contribution	Development of concepts, theories, and models	Establishment of regulatory frameworks and guidelines	Identification of best practices, lessons learned, and practical solution
Examples	Distributed systems theory, virtualization concepts	GDPR, CCPA, international data transfer regulations	Aristotile Cloud federation , OpenStack, real-world cloud federation initiatives

Purpose	Understanding the fundamental principles and frameworks	Ensuring compliance, protecting privacy and data security	Implementing and overcoming practical challenges

Although cloud federation practice is growing rapidly, it is mainly focused on research and development (R&D) projects and public services(Vaillancourt et al., 2021)(Moreno-Vozmediano, et al., 2016) (Lindpaintner, 2019; *U.S. Data Federation*, n.d.)(Birney et al., 2017; Kathryn North, 2015; Terry, 2014). In contrast, cloud federation adoption in the commercial market lags, particularly among small and medium-sized cloud providers (Haile & Altmann, 2015; K. Kim et al., 2014; Panarello et al., 2014). Cloud federation could benefit these providers greatly, but they face challenges due to limited resources, performance issues, and price competition. On the other hand, strategic alliances (federations in other sectors) have been established among SMEs to enhance their market coverage, improve competition, reduce costs, and share resources (Russo & Cesarani, 2017; Yasuda, 2005). Similarly, small and medium cloud service providers can also establish federations to address market issues (Celesti et al., 2010; Coronado & Altmann, 2017).

However, existing cloud federation practices primarily focus on non-commercial purposes, leaving a significant gap in addressing the key

elements necessary for commercializing cloud federation(Vaillancourt et al., 2021)(Moreno-Vozmediano, et al., 2016). It is essential to bridge this gap and develop cloud federation practices that specifically address the commercial market. By doing so, small and medium-sized cloud service providers can overcome resource limitations, improve performance, and compete effectively in pricing. Commercializing cloud federation would enable these providers to unlock the full potential of collaboration and resource sharing, benefiting both the providers and their customers.

Therefore, this study will investigate state-of-the-art studies using a systematic literature review to address the missing aspects from a standard document in terms of enabling factors, requirements, challenges, and current trends. In addition, the study will demonstrate a trust evaluation strategy along with a cloud federation formation algorithm to encourage a fair, inclusive, and unbiased trust evaluation for partner selection and cloud federation formation to address the issue of market concentration and vendor lock-in. By this, the study will address some of the key challenges before cloud federation can be commercialized, including a lack of standardized protocols, security concerns, and trust between partners. By this, the research will contribute to the policy and theoretical perspective on the way addressing the gaps of standard document towards establishing cloud federation and

practically will contribute to establish an inclusive, fair and unbiased cloud federation market with in small and medium cloud providers.

Chapter 3. Enabling Factors, Requirements, Challenges, and Trend Analysis of Cloud Federation Formation using Systematic Literature Review

3.1. Introduction

Cloud computing has been around for a while as a technology and service delivery model. For a long time, various industries and organizations have earned the benefits of cloud computing by storing massive amounts of data with high computational demands at low cost. The cloud providers employ a "pay as you go" model when providing various cloud computing services and charge the cloud customer based on usage. However, cloud computing provided by a single company has limited resources, so meeting all the required resources from customers is challenging. Moreover, it also has challenges regarding scalability and resource provisioning, regional workload, economic barrier, and data management. Therefore, to satisfy the cloud demand efficiently, the cloud providers can collaborate during the demand exceeding the supply or cooperate towards the same objective, and these establish the coalition of cloud providers.

The alliance of cloud providers falls into two main categories: multi-cloud and cloud federation. Multi-cloud architecture promotes the utilization of multiple distinct cloud service providers to cater to the

needs of consumers. This arrangement is governed by individual agreements with each respective cloud service provider, ensuring a seamless and tailored experience for users (Vadla et al., 2020a). In contrast to multi-cloud, cloud federation involves the interconnection and sharing of infrastructures between two or more cloud providers. Cloud federation is characterized by one cloud service provider leasing their available resources to another member within the federation. This collaborative approach allows for the efficient utilization of resources and enhances the overall performance of the federated cloud ecosystem (Lee, 2016). Differing from multi-cloud, the fundamental concept behind cloud federation is to offer seamless and transparent access to a multitude of resources and services that are dispersed across various independent providers (Panarello et al., 2014).

Cloud federation will likely take place for both commercial and non-commercial purposes due to increased service capacity and capability. However, apart from a project's initiatives, cloud federations haven’t been used in a wide range due to many reasons including interoperability, service management, contract maintenance, monitoring, orchestration, and the cloud providers' behavior. The late issue, in particular, is very much related to the partners' behavior whom the cloud providers agreed to work with. Therefore, selecting an appropriate cloud provider as a partner is crucial to the success of the collaboration.

3.1.1. Cloud Federation Formation

It is a mechanism to integrate multiple cloud service providers to cooperate towards a common objective (Aryal & Altmann, 2018; Halabi & Bellaiche, 2017). This can be achieved by signing a contract agreement between the two parties and agreeing on some common goals. Cloud federations may be formed to maximize profitability (Das et al., 2014; Das, 2015; Najm & Tamarapalli, 2022; Ray et al., 2018), minimize resource wasting and energy consumption(Aazam & Huh, 2014; Giacobbe et al., 2015), maximize resource efficiency(Pradeep Kumar & Prakash, 2019), or share knowledge (Mellaoui et al., 2021) but the important part of it is choosing the right partner to collaborate with. Apart from many challenges, studying the challenges of cloud federation formation, the general requirements for the cloud federation formation, and analyzing the existing trends will allow researchers to see the gaps and provide insight into how to solve them. Forming a cloud federation based on multiple cloud service providers which have heterogeneous infrastructure is complicated.

According to the literature, different cloud federations are formed based on different objectives as mentioned above, but some common key factors are common to all cloud federations. And these key factors need to be considered while the federation is formed.

3.1.2. Lack of Existing Review

The cloud federation domain has been reviewed from various perspectives, including cloud federation architecture, interoperability & portability, resource selection & management, and cloud federation profitability. Section 3.2 presents these review papers, which are primarily focused on review articles published after 2016. On the other hand, the review articles published before 2016 have explored the cloud federation challenges, taxonomies, and some specific requirements related to IaaS federation separately. But since then, new technologies, methodologies, and approaches have been introduced to address some of the challenges and that should also be explored and integrated with the current research findings. Therefore, this study aimed to fill this gap by exploring state-of-the-art research in the cloud federation formation discipline and identifying the current challenges to be addressed by further research. At the same time, this study will incorporate the findings from review articles published before 2016 and present them in a comprehensive way to show the currently existing gaps.

3.1.3. Goal and Contribution

Recently, research on cloud federation has mainly been conducted on the coalition formation of cloud service providers, which is the first step of any cloud federation activities. The first step towards addressing the effective and stable cloud federation formation more holistically is to explore and analyze the recently existing research in the area. The research is founded on a systematic literature review that provides a solid foundation. By reviewing the existing literature on cloud federation formation, we focused on key elements such as enabling factors, requirements, and challenges. Using a wide range of scholarly articles, we gained deep insights into the current state of the field and identified knowledge gaps. We will be able to grasp the bigger picture of cloud federation formation as a result of this comprehensive understanding of the literature. Furthermore, we employed a strategic alliance perspective in order to enhance the breadth and depth of this research. As a result, the systematic literature review was analyzed within a well-established theoretical framework based on strategic alliance theory. This perspective allowed us to assess the dynamics, decision-making processes, and potential benefits associated with strategic alliances formed through cloud federation.

Therefore, the primary goal of this study is to investigate and summarize existing studies on cloud federation formation to assist

researchers in the field by identifying gaps and providing insights for future research, as well as to assist standard organizations by identifying the major requirements to be considered throughout cloud federation formation. These will be addressed by answering the following four research questions. ***(RQ1)*** What are the enabling factors that stimulate or motivate cloud federation formation? (Section 3.4.2); ***(RQ2)*** what are the requirements that need to be fulfilled to establish cloud federations? (Section 3.4.3); ***(RQ3)*** what are the challenges that have been identified and required attention in the Cloud Federation Formation? (section 3.4.4); ***(RQ4)*** What are the latest research trends in the exploration of applied theories, methodologies, criteria influencing Cloud Federation Formation, evaluation metrics, and experimental environments utilized to measure the proposed solutions? (Section 3.4.5).

(Okoli, 2015) systematic literature review method is adapted to identify, evaluate, and synthesize research findings. This provides a concise summary of current evidence related to the research question, making it more accessible to decision-makers. Systematic literature reviews play a crucial role for several significant reasons. Firstly, they are essential for guiding and informing decision-making processes by providing a comprehensive synthesis of the available evidence on a particular topic. Secondly, these reviews help in identifying any flaws, biases, or gaps in existing knowledge, thus enabling researchers to gain

a more nuanced understanding of the subject matter. Lastly, systematic literature reviews also serve as a valuable tool in indicating areas that require further research and investigation, helping to prioritize future studies and contribute to the advancement of knowledge in the field. As scientific knowledge rapidly accumulates, reliable methods are needed to synthesize evidence like systematic literature reviews. For this, we systematically searched three databases (Scopus, web of Science, and science direct) to explore relevant studies in the area. Initially, we found 1398 studies from the three databases and after applying the inclusion and exclusion criteria, 63 relevant studies were identified for data analysis.

Based on the analysis of 63 studies, 16 enabling factors, 17 requirements, 17 challenges, and current research trends were identified. As a result of this systematic literature review, areas for further investigation of cloud federation formation are identified, such as formal institution requirements during the partner selection stage. In addition, the lack of evidence in the research methodology is highlighted as most of the study used the simulation environment, and the solution must be tested and validated in real-world cloud federation environments. By extending the state-of-the-art analysis of cloud federation enabling factors and by analyzing strategic alliances and international trade

concepts further, a new research area has been identified for knowledge creation and sharing as an enabler of cloud federation.

3.2. State of the Art

3.2.1. Overview

Cloud federation has been explored from a variety of perspectives in several review articles. As a result, we summarize the reviews and present them in two parts. The first part dealt with the review articles published before 2016, and those published after 2016 are covered in the second part. In the first section, an overview of the review articles is presented to show their focus area and how they can be incorporated into this study. The later section explains the review published after 2016 and illustrates the gap in the research by incorporating previous work and what needs to be done.

Assis & Bittencourt (2016), Petcu (2011), Toosi et al.(2014), and Grozev & Buyya (2014) are a state of the art article published until 2016, and present the motives, requirements, opportunities, and challenges of cloud federation but separately. According to Assis & Bittencourt (2016), the cloud federation architecture exhibits functional and non-functional properties. Also, Assis & Bittencourt (2016), and Toosi et al. (2014) present a motive that leads to the establishment of cloud federations along with the challenges related to interconnected clouds. The current interoperability, portability, and cloud federation challenges are

discussed in Toosi et al. (2014) and Petcu (2011). Last but not least, Grozev & Buyya (2014) present inter-cloud taxonomies, state-of-the-art approaches, and requirements. The review papers examine studies conducted before 2016, which focus on various aspects of the inter-cloud environment, a broader concept that encompasses cloud federation. Numerous papers have been published since 2016 introducing novel technologies, methods, approaches, and solutions. An overview of these papers provides an understanding of current research priorities. Therefore, in the following subsection, the topics reviewed from the studies published after 2016 are presented.

State-of-the-art articles after 2016

Review articles (2017 - 2022) concerning cloud federation are analyzed in order to identify new directions for research, summarize the information, and identify patterns among existing research studies as well as present research gaps. These reviews, which focus on specific aspects of cloud federation and are relevant to the study's objective have been selected and discussed (Table 3.1) and grouped into five categories: vendor lock-in, resource provisioning, task scheduling, profit maximization, and trust. In order to standardize and implement cloud federations, certain critical factors must be taken into account. Furthermore, these five topics address the specific dimensions of the critical factors that lead to cloud federation formation, such as enabling

factors, requirements, and challenges (Figure 3.1). Thus, these topics reflect the importance of cloud formation critical factors and are presented as follows.

3.2.1.1. Vendor Lock-in

The Kaur et al. (2018) study delves into the matter of vendor lock-in, a consequence arising from the absence of interoperability and portability, particularly concerning open standard formulation, semantics, model-driven engineering, and open libraries. Interoperability and portability serve as the primary criteria for the establishment of Cloud Federation, as they facilitate the seamless exchange and mobility of resources and services among multiple cloud providers. Over 120 papers have been reviewed and analyzed in order to analyze vendor-lock-in as one of the cloud federation motives and its challenges (Table 3.1) and suggest a variety of solutions to combat them.

3.2.1.2. Resource Provisioning

Tricomi et al. (2020) and Liaqat et al. (2017) examine approaches and challenges (Table 3.1) related to automatic resource discovery and selection from available cloud providers. It mainly deals with the cloud federation architecture and resource selection taxonomy by analyzing taxonomies, challenges, and state-of-the-art methodologies. In addition, Li et al. (2022) examine a survey of resource provisioning problems in cloud brokers. The authors analyze the resource provisioning problem by

categorizing it into resource selection problems and resource management problems using the cloud broker architecture. When implementing cloud brokers as a component of cloud federation, provisioning resources can be challenging to discover and manage in complex and heterogeneous cloud environments. Thus, the study analyzes and presents state-of-the-art approaches to resource discovery and management from various studies.

3.2.1.3. Task Scheduling

Masdari et al. (2020) differentiates between two types of inter-cloud approaches, multi-cloud and federated cloud, and present the characteristics of these two setups. It discusses intercloud scheduling schemes to allocate the appropriate virtual resources for a submitted user request. The various aspects of task scheduling have been discussed along with the current challenges (Table 3.1) in the area and possible research directions to overcome those challenges.

3.2.1.4. Profit Maximization

CongPeijin et al. (2020) focused on the profit maximization techniques for cloud federation by analyzing the method and techniques proposed by existing studies. According to the studies, profit can be increased by improving the service quality or by adjusting the price to a different level. The techniques to improve the service quality in cloud federation are by employing game theory techniques, double queue

method, using resource reservation strategy, performing resource scheduling & sharing, and providing bandwidth guarantee. Moreover, Li et al. (2022) study discussed service pricing which is another aspect to maximize profits.

3.2.1.5. Trust

Ahmed et al., (2019) focused on the issue of trust management in cross-cloud federation architecture. It explores the taxonomies, requirements, and challenges of trust management in cross-cloud federation. Moreover, it identified the multidimensional trust management system properties and requirement matrix.

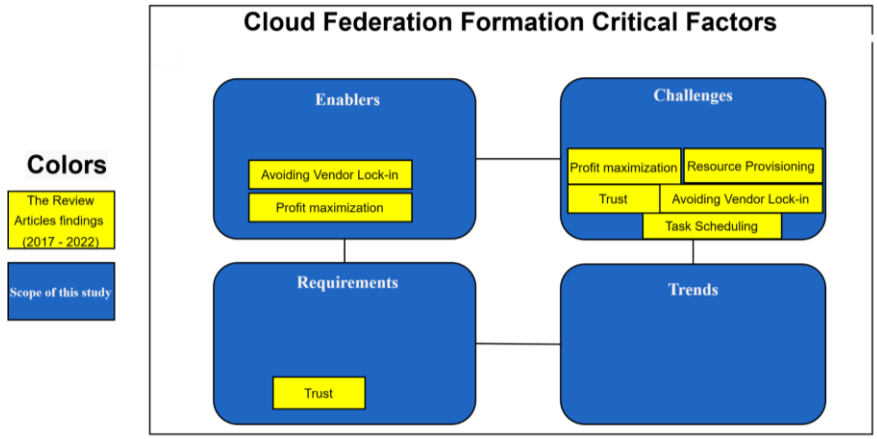


Figure 3. 1: The scope of the previous review articles (2017-2022) and the current study

3.2.2. Comparison of existing review research for identifying the research gap

The existing review articles published before 2016 address specific aspects of cloud federation formation like vendor lock-in and

profit maximization as enabling factors, trust as a requirement of cloud federation formation, and various cloud federation challenges (Table 3.1). According to the analysis (Table 3.1), the review articles focused on specific aspects of cloud federation formation. However, this study deals with analyzing the wider perspective of cloud federation formation from the standpoint of cloud federation formation enablers, requirements, challenges, and cutting-edge methodologies and techniques.

Table 3. 1: Summary of the existing review articles (2017- 2022)

Papers	Architecture		Cooperation		Focus Area	Reviewed Parameters										
	Distributed	Centralized	Multi-Cloud	Cloud federation		Taxonomy	Enabler	Requirement	Challenges	Applicable Theories	Key parameters utilized	Evaluation Method	Simulator	Evaluation factor	Comprehensive comparison	Limitation of the Studies
Zangakani (2020)		✓	✓	✓	Task Scheduling	✓			✓			✓	✓	✓	✓	✓
Li et al (2022)		✓	✓	✓		✓			✓						✓	✓
Kaur et al(2018)	✓	✓	✓	✓	Vendor Lock-in (Interoperability)	✓	✓		✓			✓	✓		✓	✓
Li et al (2022)		✓	✓	✓	Resource Provisioning	✓			✓						✓	✓
Tricomi et al (2020)	✓		✓	✓		✓			✓			✓		✓		✓
Liaqat et al (2017)	✓	✓		✓		✓			✓			✓	✓	✓		✓
CongPeijin et al (2020)		✓		✓	Profit Maximization	✓	✓		✓			✓		✓	✓	✓
Ahmed et al (2019)	✓	✓	✓	✓	Trust Evaluation	✓		✓	✓			✓			✓	✓
This Study	✓	✓		✓	Coalition Formation (Broader Perspective)		RQ1.	RQ2.	RQ3.	RQ4.	RQ4.	RQ4.	RQ4.	RQ4.	✓	✓

In order to gain a comprehensive understanding of cloud federation implementation, it is imperative to understand the factors driving federation establishment, the requirements for federation, and the challenges involved. Although previous reviews provide valuable insight into a variety of topics, including vendor lock-in and profit maximization as enablers, trust as a requirement of cloud federation formation, and some of the challenges associated with it, this study examines cloud federation formation from a broader perspective. Interoperability is discussed as a means of addressing vendor lock-in issues, as well as profit maximization techniques, in studies by Kaur et al. (2018) and CongPeijin et al. (2020). Based on previous studies, these two factors enable the formation of cloud federations. Regarding the requirements for cloud federation formation, only the trust aspect is discussed in detail by Ahmed et al. (2019). Prior research (2017 - 2022) has not systematically examined the enabling factors and requirements of cloud federation.

Therefore, this study aimed to fill this gap by addressing the wider aspects of enabling factors and requirements. This study assists cloud provider managers to make better and more timely decisions by exploring and presenting the possible motives and enabling factors for cloud federation formation. Furthermore, the study explores the necessary conditions and requirements that must be fulfilled before cloud

federation formation to guide expertise in this area. This study also serves as a reference for standardizing and implementing cloud federation. On the other hand, previous reviews (2017 - 2022) have discussed the challenges of cloud federation formation. Resource selection and management Tricomi et al. (2020) Li et al. (2022), service pricing by Li et al.(2022), trust by Ahmed et al.(2019), interoperability by Kaur et al. (2018), profit maximization CongPeijin et al. (2020) and task scheduling by Masdar & Zangakani (2020) are the topics covered by the review articles. Taking a broader view, this study analyzes recently published research (2016-2022) that explores different aspects of cloud federation formation. Hence, experts and researchers can gain an understanding of the challenges explored in the literature, and the state-of-the-art approaches used to address the challenges, and practitioners, at the same time, can get an understanding of the main enabling factors and requirements for cloud federation in order to make a good decision on time. This is because there is no recent comprehensive review of cloud federation enabling factors, requirements, challenges, and current trends (Table 3.1), which this study addresses the gap by answering the following four research questions.

***RQ1**: What enabling factors stimulate or motivate cloud federation formation?*

RQ2: *What are the requirements that need to be fulfilled to establish cloud federations?*

RQ3: *What are the challenges that have been identified and required attention in the Cloud Federation Formation?*

RQ4: *What are the latest research trends in the exploration of applied theories, methodologies, criteria influencing Cloud Federation Formation, evaluation metrics, and experimental environments utilized to measure the proposed solutions?*

Answering these questions provide insights into the current state of research on cloud federation formation, including the enabling factors that motivate cloud federation formation, the requirements that must be addressed to establish cloud federations, the challenges that must be overcome to create successful federated cloud environments, and the current trends and solutions proposed by recent studies. These insights can be valuable to researchers and practitioners in cloud computing, as they can help to guide future research and development efforts, inform decision-making related to cloud federation formation, and provide a foundation for the creation of best practices and standards in this area. Additionally, understanding the current state of research on cloud federation formation can help to identify gaps in knowledge and areas where further research is needed.

3.3. Methodology

A systematic literature review is a clearly outlined approach to systematically identify, assess, and comprehend all pertinent studies centered on a particular research query, subject domain, or noteworthy phenomenon. Consequently, this technique is employed to impartially, credibly, and objectively assess methods that contribute to shaping the establishment of cloud federation. Before conducting the SLR, small research is performed to explore an appropriate methodology from various SLR proposed by different authors. Among those, the methodology proposed by (Webster & Watson, 2002) and a methodology proposed by Okoli (Okoli, 2015) are compared to choose the appropriate methodology. Compared to the methodology proposed by (Webster & Watson, 2002), Okoli's methodology develops a custom design methodological approach for IS domain researchers by providing a guideline of SLR that includes the contribution from social sciences (Petticrew & Roberts, 2006), health sciences, software engineering (Kitchenham et al., 2015) and, management and organization science.

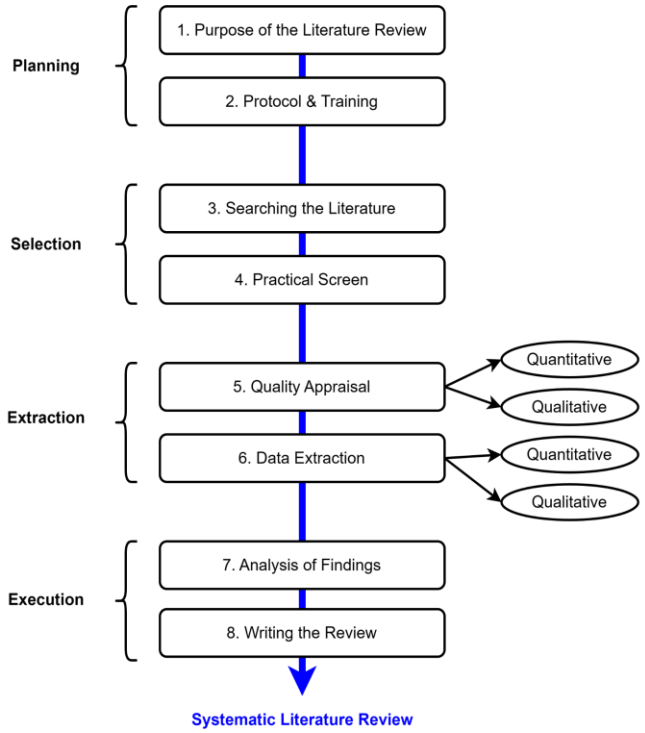


Figure 3. 2: Steps of the SLR to be conducted (Adapted from (Okoli, 2015))

Since the guideline incorporates best practices from various fields, it provides a well-balanced strategy to incorporate both quantitative and qualitative approaches. Furthermore, this methodology is used for doing the literature review since it recognizes the difficulties of doing SLR successfully. Therefore, Okoli's method is adapted in this research. The Okoli's SLR, consists of eight rigorous stages as shown in Figure 3.2.

3.3.1. Planning

The goal of this study is to explore the enablers, requirements, challenges, and trends of Cloud Federation formation from primary

studies and analyze their findings. In order to explore what has been done, the previous review papers are analyzed and summarized (Table 3.1). Consequently, a research question is formulated based on the gaps identified in the review paper's analysis and findings. In order to ensure rigor and repeatability, SLR starts by developing a review protocol. Using Okoli's guidelines, we designed the review protocol and searched the literature directly.

3.3.2. Selection

We used automated searches from three databases: Scopus, Web of Science, and Science Direct using the searching syntax (Table 3.2) and target to explore the conference proceedings and journal papers. The study type such as empirical analysis, theoretical study, mathematical and/re experimental analysis are included because of the complexity of identifying the standard study type in our problem domain.

3.3.2.1. Search Strategy

Based on the methodology by Okoli (Okoli, 2015), the first stage is to perform an automated search based on the given keyword in the above section. According to keyword analysis, the 12 keywords are identified as alternative keywords for cloud federation. This means that the 12 keywords combined with the other 6 keywords to formulate 72 combinations of searching keywords. Using these 72 searching

keywords, three databases are explored and the resulting number of papers was observed as shown in the following table.

Table 3. 2: Searching keywords for each databases

Database	**Searching syntax**	**Number of papers**
Science Direct	(("Cloud federation*" OR "federated cloud*" OR "federation of cloud*" OR "cloud provider coalition*" OR "federated cloud computing*" OR "cloud service provider coalition*") AND form* OR create* OR establish*)	667
Scopus	TITLE-ABS-KEY (("Cloud federation*" OR "federated cloud*" OR "federation* of cloud*"OR "cloud provider* coalition*" OR "federated cloud computing*" OR "cloud service provider* coalition*" OR "inter cloud*" OR Inter-cloud) AND form* OR create* OR establish*)	512
Web of Science	ALL = (("Cloud federation*" OR "federated cloud*" OR "federation* of cloud*"OR "cloud provider* coalition*" OR "federated cloud computing*" OR "cloud service provider* coalition*" OR "inter cloud*") AND (format* OR Creati* OR establish*))	219

3.3.2.2 Practical Screening

Accordingly, the first query given the combination of keywords, three databases are explored. As shown in the above table, the total number of papers identified given the keyword combinations is 1398 papers. This result is before applying any kind of inclusion and exclusion criteria.

Inclusion Criteria

1. The inclusion criteria for the literature search are studies published between 2016 and 2022.
2. Only studies with a substantial emphasis on Cloud Federation Formation will be considered.
3. Studies included in this review must have been published in peer-reviewed sources and have their full text available in English.
4. Studies published as conference proceedings and journal articles
5. Studies that are relevant to the objective of the study.

Exclusion Criteria

1. Studies other than that Conference and Journal papers
2. Research that examines cloud federations but does not specifically focus on coalition formation (establishing cloud federations).
3. Studies that were not published in English or peer-reviewed

4. Reports, Book chapters, Books, presentation materials, and posters
5. Dissertations, books, posters, presentation materials, and review articles
6. Studies published before 2016

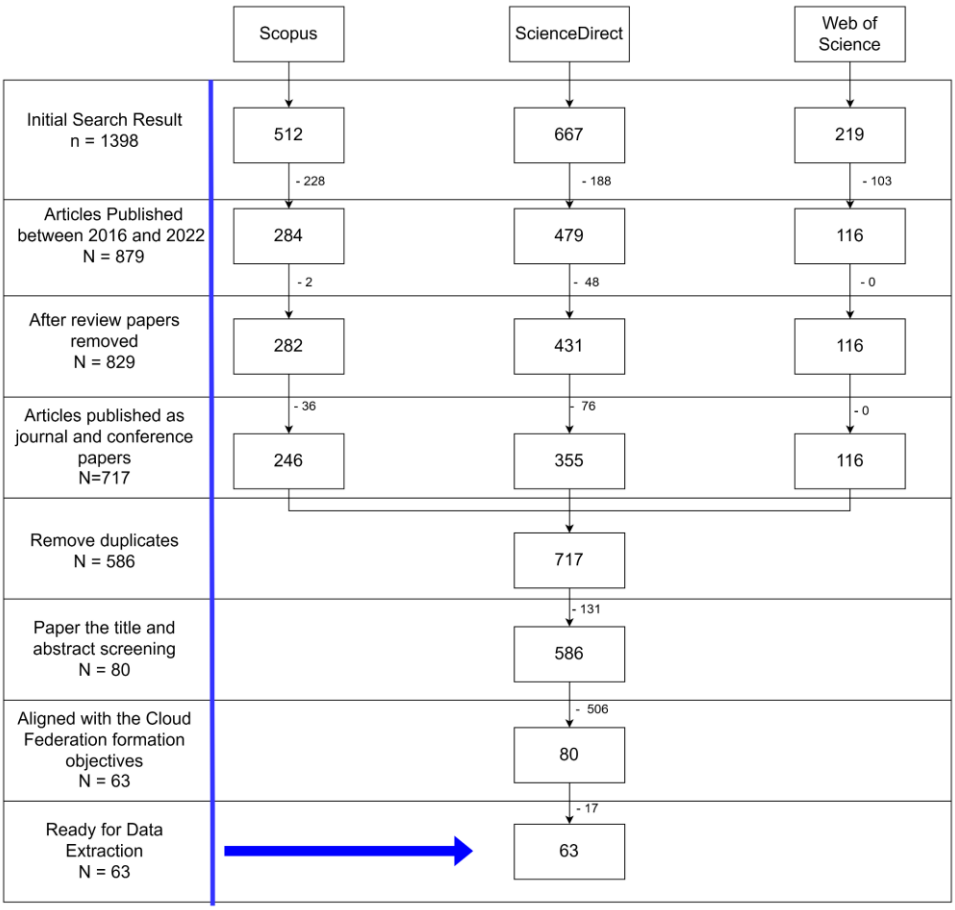


Figure 3. 3: papers selection procedure

After applying the inclusion and exclusion criteria, the number of papers is reduced to 63 papers.

3.3.3. Data Extraction

The data extracted from the study were presented as follows:

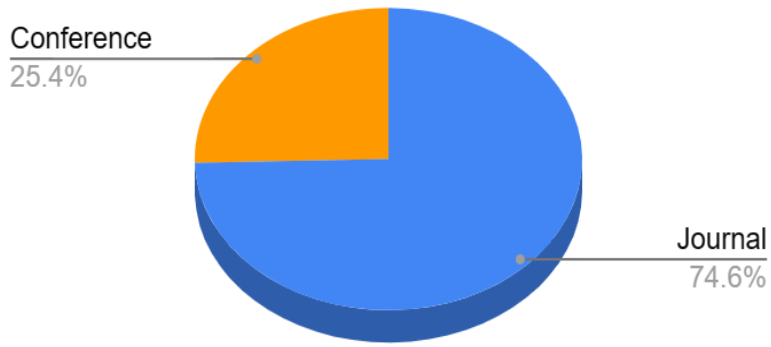
- References and the source (journal or conference)
- Study topic
- The author(s) and their institutional affiliation
- Publication year
- The publisher's organization
- The study's abstract
- Purpose and summary of the study
- Key data to answer the research questions (RQ1 - RQ4 (including proposed solution by the authors, simulation environment, and methodology utilized by the study))
- Quality evaluation

Quality appraisal is conducted concurrently with data extraction. Six screening questions were adapted from the Kitchenham quality appraisal guideline (Kitchenham et al., 2015). A quality appraisal score of 30 was taken, and all the studies passed the evaluation with quality measures exceeding 50% of the total score. The retrieved studies are documented, managed, and organized using Zotero version 5.0.96.3. The findings are extracted from a Google spreadsheet shared between team members.

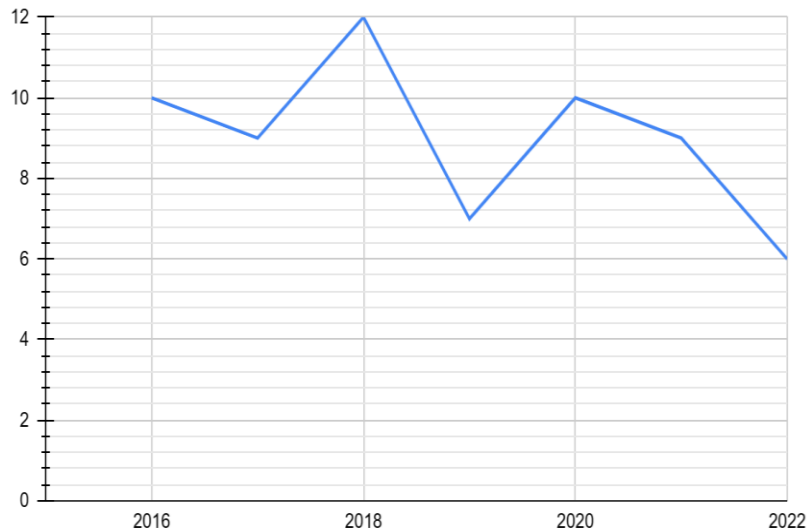
3.4. Analysis

3.4.1. Descriptive Analysis

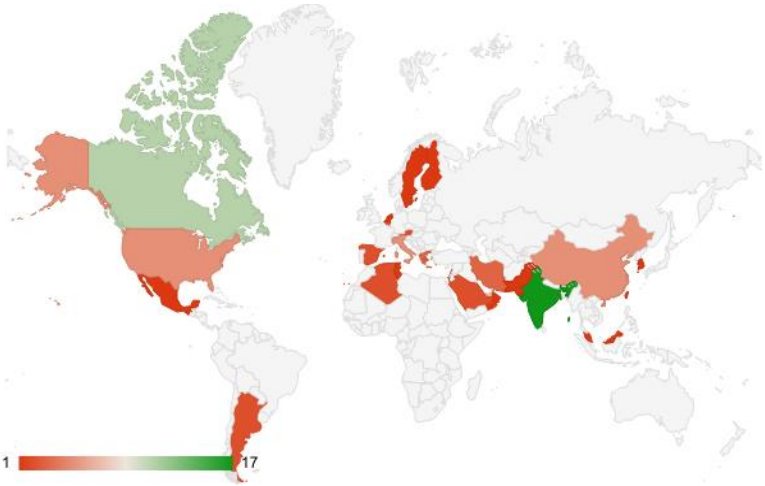
The data extraction process of the study involved the selected 63 studies for analysis. Out of these 63 studies, 74.6 percent are journal papers (Figure 3.4. (a)), which are peer-reviewed and published in reputable academic journals (Table 3.3). The remaining studies are conference papers. Figure 3.4.a. presents the distribution of the 63 selected studies between journal papers and confidence papers. This figure shows that a majority of the studies used for analysis are journal papers, which indicates that the research team may have placed greater emphasis on using high-quality and peer-reviewed sources.



a)



b)



c)

Figure 3. 4: a) Percent of journals and conferences from the selected studies b) number of studies per year of publication c) Papers Demographic information

Figure 3.4 (b) and Figure 3.4 (c) show the distribution of studies based on their publication year and demographic information, respectively. Figure 3.4 (b) provides information on when the selected studies were published, which can help identify trends and changes in the field over time. Figure 3.4 (c) provides information on the demographics of the studies, which can help identify patterns and variations in the data based on different factors such as geography.

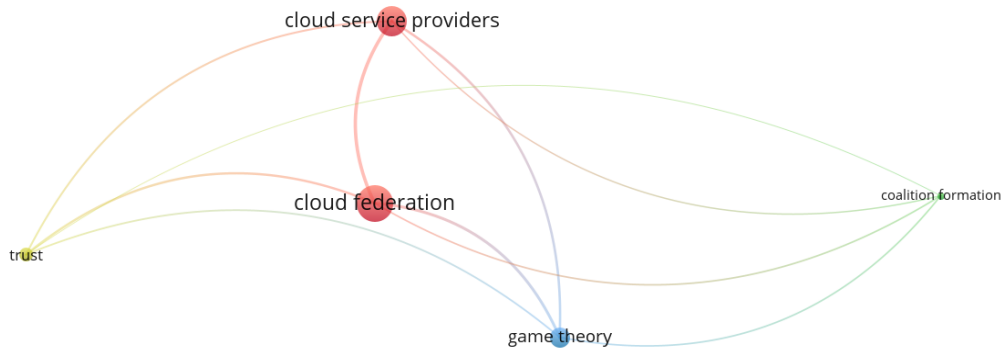


Figure 3. 5: Keyword Clusters

The article's keywords are used to identify the main topics and themes discussed in the article. By examining how these keywords are related to each other, the researcher can gain insights into the structure and content of the article. The researcher used VoSviewer to identify keywords that occurred at least 5 times in the article. This threshold was chosen to focus on the most important and frequently discussed topics in the article. Based on these 5 keywords, the researcher used a fractionalization method to identify 4 clusters of related keywords (Figure 3.5). The fractionalization method is a technique that groups similar keywords together based on their co-occurrence in the article. This technique helps to identify patterns and relationships between keywords that may not be immediately apparent.

Table 3.3: Number of studies per publisher

Publisher	Total Number of papers	Journal	Conference
IEEE	22	11	11
SpringerLink	16	12	3
ELSEVIER	8	9	0
Wiley Online Library	4	4	0
Inderscience Enterprises	2	2	0
Emerald	1	1	0
IGI Global	1	1	0
Informatics India Ltd.	1	1	0
Little Lion Scientific	1	1	0
MDPI	1	1	0
Research India Publications	1	1	0
Taylor & Francis	1	1	0
UPM	1	1	0
World Scientific	1	1	0
Others	2	0	2
Total	**63**	**47**	**16**

3.4.2. Cloud Federation Formation Enabling (Driving) Factors

To answer the first research question (*RQ1, What are the enabling factors that stimulate or motivate cloud federation formation?*), the studies were reviewed by extracting the keywords and phrases from

the articles dealing with the motives of establishing cloud federation. The similarity and complementarity of these keywords are carried out to group them accordingly and to associate the results with the previous review articles published before 2016. As a result, **16 enabling factors** are identified after the categorization process, and among those 9 of them are identified in the previous review article. These factors namely, Resource Provisioning and Elasticity, Economic Barriers, Regional Workload(Large demand), Cost Efficiency and Saving Energy, Availability & disaster recovery Scalability & Dynamic Capability, Geographical Distribution & Low network latency access, Interoperability & Avoid Vendor lock-in, Legal Issue & Meeting the Regulation, Enhance Sharing Economy, Improve QoS, Security Privacy & Single Sign-on, Prevent SLA violation & maintain the client's requirement, Reliability & Transparency, Visibility & Replica, and Heterogeneity & Value added service. Earlier review articles published before 2016 identified and supported the prior nine enabling factors (orange color), but the last 7 enabling factors (blue color) are new factors identified in this study.

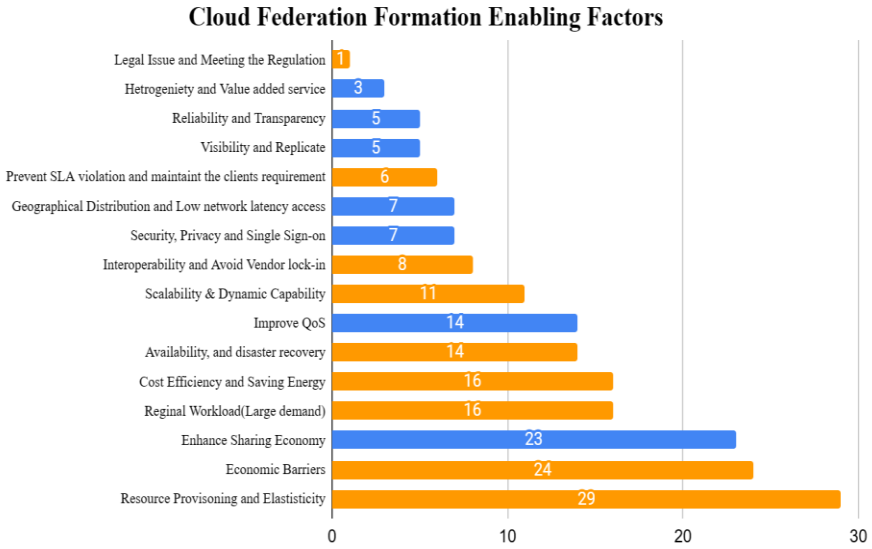


Figure 3. 6: Cloud Federation enabling factors (motives)

The main objectives of cloud service providers are to accommodate all the resource requests from clients, utilize the resources efficiently, and maximize their revenue. Taking this into account, more than 46 % of studies show that resource provisioning and elasticity(Abusitta et al., 2018; Ayachi et al., 2021a; Biran & Dubow, 2019a; Comi & Fotia, 2018; Darzanos et al., 2019a; Dhole et al., 2016a; Dinachali et al., 2022; Hadjres et al., 2020a; Halabi et al., 2018; Hammoud et al., 2018a, p. 31, 2020a; Hassan et al., 2016a; Khandelwal et al., 2016a, 2018a; Kirthica & Sridhar, 2018; Latif et al., 2021; Y. Li et al., 2022; Massonet et al., 2016, p. 11; Mourougan & Aramudhan, 2016a; Pacini et al., 2019; Panarello et al., 2016; Ray et al., 2019; Shrivastava & Pateriya, 2020a; Suzic & Reiter, 2016; Thomas & Chandrasekaran, 2017; Wahab et al., 2018a; Xu & Palanisamy, 2021) as one of the

enabling factors of cloud federation formation. Insufficient infrastructure and technology prevent efficient resource utilization and underutilization of computing resources. Moreover, joining the cloud federation would allow the cloud service provider to rent computing resources from foreign cloud service providers and optimize global resource usage without building new points of presence. As a result, the user gets fast service without interruption while reducing resource stress.

Overcoming economic barriers is the second most discussed enabling factor(Ayachi et al., 2021a; Biran & Dubow, 2019a; Bouchareb & Zarour, 2021; Comi et al., 2016a; Darzanos et al., 2016a; Dhole et al., 2016a; Dinachali et al., 2022; Farris et al., 2017a; Hammoud et al., 2020a; Khandelwal et al., 2016a, 2018a; Latif et al., 2021; Y. Li et al., 2022; Mashayekhy et al., 2021a; Moghaddam et al., 2020a; Nemati et al., 2019a; Ray et al., 2021a; Romero Coronado & Altmann, 2017a; Shrivastava & Pateriya, 2020a, p. 3636; Vadla et al., 2020a; Wu et al., 2022; Xu & Palanisamy, 2021). Approximately 38% of the studies examine motives that aim to maximize the utility of CPs and global social welfare. These motives include: generating additional economic benefits, maximizing cloud service provider profits, increasing external competition, gaining access to economies of scale, improving user quality of life, and creating a market that is competitive rather than monopolistic. In addition, cloud providers' incentives are another

enabling factor. Further analysis is done for the cloud federation formation enabling factors to explore the proactive and reactive nature (Table 3.4). It helps the audience to better understand and use it as a reference to make a decision on the circumstances that require deciding whether the cloud federation needs to be established or not.

Table 3. 4: Proactive and reactive nature of the cloud federation formation enabling factors

Enabling factors	Scope of the factors	Proactive Nature	Reactive Nature	Paper ID (Appendix 1)
Resource Provisioning and Elasticity	The need for Resource scaling capability	✓		(29 Articles) P5,P7-P8,P10-P11, P14, P18-P21, P31, P34-P39, P41-P43, P46-P47, P49-P50, P57-P58, P60-P62)
	The need for extra resource		✓	
	Lack of infrastructure and technology (Resource Capacity constraints)		✓	
	To allow a more efficient resource usage	✓		
	To Outsource and utilize the idle (underutilized) resource	✓		
	To manage unprecedented resource demand		✓	
	Automated service function chaining across datacenters	✓		
	To increase efficient resource utilization	✓		
	To satisfy the users resource demands		✓	
	To tackle over-provisioning the available resource		✓	
Economic Barriers	For better QoE	✓		(24 Articles) P15-P16, P19, P22-P23, P25, P28, P31, P33, P35-P38, P42-P43, P46, P50, P52-P53, P55-P57, P59, P60)
	To maximize the customers utility	✓		
	To maximize the cloud service provider's social welfare	✓		
	To Generate extra revenue	✓		
	To gain Access to economy of scale		✓	
	To cloud service provider strategic behavior		✓	
	To improve the cloud service provider	✓		

	Utilities			
	To incentivize cloud service providers		✓	
	To attain external market Competition		✓	
Enhance Sharing Economy	To share computing resource	✓	✓	(23 Articles) P1, P3-P4, P7, P13, P15-P19, P26, P29, P35, P39, P41, P44, P45-P47, P49, P59, P62-P63
	To share Information	✓		
	To dare Data	✓		
	To share knowledge	✓		
	To facilitate efficient resource sharing	✓		
Regional Workload(Large demand)	To Outsourcing the workload		✓	(16 Articles) P1-P2, P16, P21, P25, P28, P31, P34, P37, P41-P42, P48, P53, P56, P58, P61
	Task Deadline Constraints		✓	
	To prevent customers from service rejection		✓	
	To increase the capacity of handling large requests	✓		
	To maintain Regional workload distribution	✓		
	To manage unprecedented resource demand		✓	
Cost Efficiency and Saving Energy	To reduce the deployment cost	✓		(16 Articles) P6, P16, P19, P22, P25, P31, P36-P38, P40-P41,P46, P49, P52-P53, P59
	To reduce energy costs by exploiting electricity price fluctuations across different locations		✓	
	To lower energy consumption		✓	
	To reduce the stress on resource		✓	
	To reduce operational cost		✓	
	For cost effective service delivery	✓	✓	
Availability, and disaster recovery	To improve service availability	✓		(14 Articles) P2, P6, P8, P10, P12, P16, P25, P37, P40, P46, P48, P50, P58, P61
	To prevent system interruption in case of natural disaster	✓		
	To prevent from unexpected system failure	✓		
	To enhance resilience of system failure	✓		
	To ensure the adequate service responsiveness	✓		
Improve QoS	To maintain the promised QoS (during the sudden spikes in the resource demand)		✓	(14 Articles) P5-P6, P8-P9, P13, P16, P34,
	To improve the QoS management	✓		

	To increase level of performance	✓		P42, P46-P47, P50, P55, P59, P60
	The need of high efficient system (service)		✓	
	To provide better service to the customer	✓		
Scalability & Dynamic Capability	The need for resource scaling capability		✓	(11 Articles) P2, P8, P10, P18, P20, P27, P30, P40, P46, P52, P59
	The need to offer high end and flexible service	✓		
	Increase dynamic capability	✓		
	Automated service function chaining across datacenters	✓		
Interoperability and Avoid Vendor lock-in	To avoid (reduce) the vendor-lock in risk	✓		(8 Articles) P1,P2,P24,P28,P29,P34, P35, P55
Security, Privacy and Single Sign-on	To provide a single sign-on service	✓		(7 Articles) P5, P10, P14, P27, P35, P38, P44
	To enhance the user authentication process	✓		
	To reduce service complexity	✓		
	To enhance security and privacy of cloud service provider	✓		
Prevent SLA violation and maintain the clients requirement	To prevent from SLA violation		✓	(6 Articles) P1, P28, P36, P54, P56, P58
	To accommodate the SLA (Service Level Agreement) requirements from client		✓	
	To minimizing the penalties incurred by violated SLAs		✓	
Geographical Distribution and Low network latency access	To improve the service delay		✓	(7 Articles) P6, P8, P18, P25, P47-P48, P61
	To ensure adequate responsiveness	✓		
	Expand geographic footprint	✓		
	To creating a distributed infrastructure to effectively process data generated	✓		
	To guarantee performance		✓	
Reliability and Transparency	To enhance trust between cloud service provider and Client	✓		(5 Articles) P12, P27, P35, P59, P63
	To create transparency (for the user)	✓		
	To improve the reliability	✓		
Visibility and Replicate	To expand and enhance service visibility	✓		(5 Articles) P5-P6, P25, P44, P47
	To replicate computing resources	✓		
	To replicate and store data	✓		
	To maintain data security	✓		
Heterogeneity	To accommodate heterogeneous task		✓	(3 Articles)

and Value added service	request from user			P25, P34, P36
	To maintain the demand of Service variety		✓	
	To enable Value-added services	✓		
	To increase their Business prospects	✓		
Legal Issue and Meeting the Regulation	Legal Issue	✓	✓	(1 Article) P61

3.4.3. Cloud Provider's Requirements for Establishing Cloud Federation

The second research question (*RQ.2. What are the requirements that need to be fulfilled to establish cloud federations?)* is to answer the requirements of cloud federation addressed by the studies. The studies explore **17 requirements** in different contexts. The trust and reputation requirement (59%) is the most addressed requirement in the cloud federation formation. The trust between cloud providers with other cloud providers and the trust between cloud providers with cloud federation entities are the scope of the studies.

Second, the most frequently explored requirements are availability & stability requirements (27%) followed by SLA & FLA terms requirements before establishing or joining cloud federations (Figure 3.7).

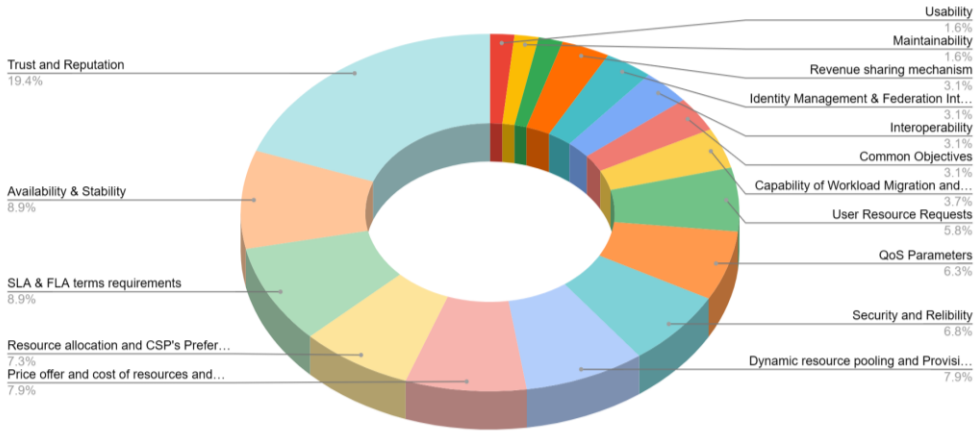


Figure 3. 7: Requirements for cloud federation formation

Since the formation is the beginning stage, a few stakeholders namely cloud service providers and cloud federation brokers are involved in the activities. The cloud service provider is responsible for choosing suitable partners and the cloud federation broker is responsible for managing and facilitating activities from the federation side. Therefore the requirements of cloud federation formation distribution with respect to these to stakeholders show that the Trust between cloud service providers is the main requirement from the cloud service providers' side, followed by Availability & stability of cloud service provider and the SLA & FLA agreement terms are the highly explored requirements from the studies. From the Cloud federation broker side, the capability of workload migration and live transmission is the highest priority of requirements followed by the cloud service provider revenue & profit-sharing mechanism.

Requirement 1 (Trust and Reliability): Since data and resources are protected by the cloud provider, a strong trust relationship is essential. A cloud service provider must establish trust with another provider as well as the central federation broker before sharing resources.

***Requirement 2 (Availability and Stability)*:** cloud service providers must be responsive to their customer's demands, stable, and open to federation with other providers to maintain their share of the competitive advantage in the Cloud market.

***Requirement 3 (SLA and FLA terms)*:** In order to ensure the future quality of services, cloud service providers need to agree on SLA parameters, policies, and rules so that federation members can reach a consensus that guarantees the promised quality of service as well as economic sustainability for the federation and the cloud service providers.

Requirement 4 (Resource allocation requirements and cloud service provider preference): The cloud provider's allocation requirements and preferences containing participant identification and QoS information for the required VM, and available network information must be determined before the federation can be established.

Requirement 5 (Price offer and cost for resource and energy consumption): Participants are required to provide their resource capacity, energy consumption costs, operation costs, penalty rate, QoS-

dependent pricing, and other cost-related rules and regulations so that each provider can set a price that does not violate federation participation rules.

Requirement 6 (Dynamic resource pooling and provisioning): Achieving the promised QoS requires dynamic resource pooling capability and optimal resource provisioning that allow providers to dimension their resources and fulfill the required QoS. The Monitoring aspect becomes an increasingly important part of any Federated Cloud as it provides a consistent stream of up-to-date information about the resources within a system, which is crucial for giving the scheduler an accurate picture of the system's resources.

Requirement 7 (Security and Reliability): Before transferring sensitive data outside of secure environments, it is crucial to mask or encrypt the data to ensure its protection. Additionally, it is essential to separate the security requirements for the cloud providers' manager from those of the federation manager. These security requirements must then be translated into appropriate security policies for each layer: the Cloud and federation manager layers. To ensure the security of data in transit and data at rest, the integrated cloud management system must be both secure and reliable at each layer. Moreover, it is essential to establish a secure collaboration environment with all the necessary security measures in place to safeguard the data effectively.

***Requirement 8 (QoS Parameters)*:** QoS satisfaction is measured using the QoS parameters, so it is important that rules and regulations are established regarding QoS before the federation is established.

Requirement 9 (User resource request): Services and resources that couldn't be fulfilled by a single provider are needed to join or establish the cloud federation in the first place.

Requirement 10 (Capability of Workload Migration and Live transformation): One service provider needs to be able to migrate fully-stopped virtual machine instances, machines, or container images to another service provider through the cloud federation, as well as migrate applications and services. Therefore, it is essential for cloud providers and federations to allow workload migration and live transformation.

Requirement 11 (Common Objectives): Cloud federation brings together cloud providers with common interests. Therefore, it is essential for cloud providers to be like-minded or have the same domain of interest to be able to cooperate and deliver services as a cloud federation.

Requirement 12 (Interoperability): Irrespective of the specific hardware and technology utilized, it is imperative that applications and services are capable of operating on the diverse infrastructure provided. Furthermore, the cloud provider must be prepared to accommodate a transaction with the designated cloud, resulting in an augmented allocation of resources for the user. Consequently, the crucial demand

for cloud providers is to ensure interoperability, enabling seamless interaction and compatibility among different systems and services.

Requirement 13 (Identity Management and Federation Interface)*:* To scale existing authentication systems to the cloud, a significant effort such as identity management is required. Furthermore, any cloud provider who wishes to be a part of a cloud federation must have a federation interface (which permits interaction with external resources) or API (a connector that translates common requests into specific commands).

Requirement 14 (Revenue Sharing Mechanism): Among the reasons why cloud providers join federations is to maximize their profits. Cloud providers must ensure that joining the federation will earn them extra revenue, and revenue sharing is another element they must consider before joining the federation.

Requirement 15 (Common Standard requirement): It is necessary for cloud providers to have a uniform way of managing all data transactions, and storing data in order to achieve their common objectives. As well, there are necessary requirements for cloud federation (such as data protection, security, and other necessary standards and protocols).

Requirement 16 (Maintainability): A cloud-based system must be designed and developed so that it can be effectively maintained, with the least amount of service disruption, and with the least amount of operating

costs. This is a key requirement for cloud service providers to be innovative as well since an effective design will eliminate the need for break-in periods that can destabilize cloud providers' services.

Requirement 17 (Usability): Ensuring effective system usability goes beyond hardware or software design alone. Cloud service providers must prioritize operability to deliver an efficient and user-friendly service. One of the primary motivations for creating cloud federations is to prevent vendor lock-in, allowing users the freedom to choose among different providers. However, each cloud service provider offers specific tools and standards for deploying, maintaining, and monitoring workloads, which are not standardized across all providers. This lack of standardization makes usability suboptimal for users aiming to operate in a multi-cloud service provider architecture, as they must adopt various tools from different providers. To establish an effective cloud federation, usability becomes a critical factor for cloud service providers. By focusing on user-friendly interfaces and standardized tools that work seamlessly across multiple providers, cloud service providers can enhance the usability of their services and foster a more efficient multi-cloud environment. This, in turn, contributes to the overall success and adoption of cloud federations, promoting a flexible and user-centric cloud ecosystem.

3.4.4. Addressed Cloud Federation Formation Challenges

Next, we will examine challenges in the formation of cloud federations in order to answer the third research question (***RQ3:*** *What are the challenges that have been identified and required attention in the Cloud Federation Formation?*). Although the challenges are diverse and wide, It has been simplified to **18 challenges** as shown in the figure below. Some of the challenges are addressed from the cloud federation broker's perspective and the individual cloud service providers' perspectives. The details of each challenge are discussed in the following sections.

3.4.4.1. Cloud Federation Stability

Providers' stability depends on their ability to be stable individually. There are a number of strategies employed to address the stability issue, like the Nash stability, Individual stability, or Core stability

Cloud Federation Broker: stability challenges in cloud federation have many aspects. The stability of cloud federation itself is just one of these challenges. Literature uses an optimal allocation algorithm or a scalability algorithm to create a stable federation. How the coalition is cloud federation stability, stability of coalition partition of providers, Pareto optimal allocation strategy, envy-free allocated shares of items, convergence to Nash stable solution,

Cloud Service Providers: the stability of individual providers affected by the provider's opportunistic behavior or performance stability.

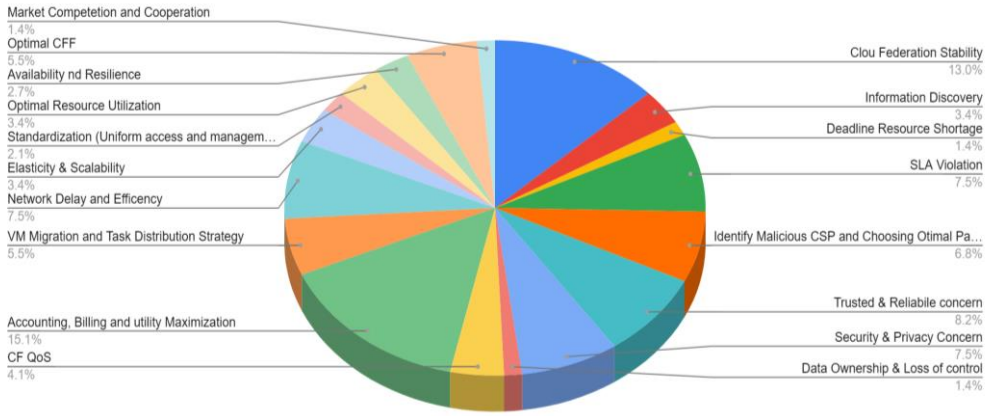


Figure 3. 8: Cloud Federation Formation challenges

3.4.4.2. Information discovery (Dynamic Updating of Cloud Service Provider (Resource Scale up & down) context

Discovering the information about the cloud service provider is another challenge addressed by literature. Information including dynamic updating and the current status of cloud service providers' resources during the time of resource scale-up or scale-down. This information is crucial to allocate tasks and workload to appropriate cloud providers and to ensure the assigned job to each cloud provider doesn't exceed the current cloud provider's capacity.

3.4.4.3. Deadline Resource Shortage

For The deadline resource shortage, ensure that each cloud service provider in the federation is assigned at least one job, and ensure that the assigned jobs to each cloud provider do not exceed the cloud provider's capacity.

3.4.4.4. SLA and FLA Violation

Due to the large surge in demand from consumers during peak hours, denial of service and SLA violations can occur. Reducing this

issue is crucial to the success of cloud federation. A study shows that reducing SLA violations and severity is also a challenge that can be overcome by enhancing negotiation techniques that minimize the possibility of SLA violations and eliminating providers who are unreliable.

3.4.4.5. Identify Malicious Cloud Service Provider and choose optimal partner

Identification of a reliable cloud service provider is essential to establish a stable cloud federation. Literature explores the challenge of identifying malicious or ineligible cloud service providers that could negatively affect cloud federations. The studies offer different strategies on selecting optimal cloud service provider, minimizing the number of malicious providers, and maximizing the possibility of identifying them.

3.4.4.6. Trust & Reliability concern

To form a cloud federation, trust is a crucial requirement, and achieving a high level of trust has been a challenging task. The selection of reliable and trustworthy cloud providers is one of the challenges encountered during cloud federation. Obtaining high levels of trust between the home cloud and the foreign cloud is also another challenge identified by the studies. Studies provide strategies to eliminate cloud providers with bad reputations, or unreliable cloud providers in order to address these challenges.

3.4.4.7. Security & Privacy Concern

In the literature, it has been observed that security and privacy concerns are a challenge for both cloud providers and cloud federations.

Cloud Federation Broker: In order to establish a cloud federation, the cloud federation must provide authentication and authorization services including enhanced user authentication.

Cloud Service Providers: The performance and security of a cloud federation could be enhanced by the security measures taken by cloud providers. This includes techniques to reduce the possibility of attacks on data, to ensure data confidentiality, or to detect fewer breaches.

3.4.4.8. Data Ownership & Loss of control

Another issue addressed in the literature is how to give cloud providers control over their own data while allowing them to share infrastructure across organizational boundaries. In particular, during workload migration, data ownership and control should be clearly determined and issues should be addressed. This will increase provider stability and increase trust between federation members.

3.4.4.9. Cloud Federation QoS

Cloud Federation Broker: Optimizing QoS and performance, and ensuring a global QoS that is close to optimal are a few of the challenges explored in the primary study results.

Cloud Service Providers: A loss of performance on the part of individual cloud service providers, resulting in performance degradation on the part of the cloud federation and additional performance costs for them.

3.4.4.10. Accounting, Billing, and Utility Maximization

In cloud federation formation, the economics-related issue is the first challenge widely explored.

Cloud Federation Broker: It is about making cloud federation as profitable and efficient as possible while maximizing its utility and social

welfare as well as minimizing average social costs. Further, the company's strategy to reduce network access costs, VM migration costs, cost optimization, and a profit-sharing policy are significant aspects of formation. Studies have provided various solutions to address these issues as a major challenge in cloud federation formation.

Cloud Service Providers: Using a cloud service provider utility maximization strategy, each member of the federation should consider how to maximize their individual satisfaction, fair profit maximization, fair payout distribution, minimize the penalty cost as well as the average welfare distribution among all members.

3.4.4.11. VM Migration and task distribution Strategy

To migrate tasks or VM instances across providers, task allocation and VM migration are essential. In the studies, VM migration or task (workload) distribution strategies were mentioned as being challenging. The study looked at several issues, including migration strategy, efficient task forwarding strategy, assessing overall workload, and ensuring that task assignment and execution of the assigned task do not exceed the deadline for each cloud provider.

3.4.4.12. Network Delay and Efficiency

Several studies identify the delay in network communication as another issue, including the delay in cloud federation formation execution time, the total VM migration time, the execution and response time of individual cloud service provider resources, as well as the latency of individual cloud service provider resources.

3.4.4.13. Elasticity & Scalability concern

Another issue examined in the study is a strategy intended to address elasticity and scalability to overcome the elasticity and scalability issue in a cloud federation. A strategy for resource elasticity and scalability needs to be defined and agreed upon by all the members of the cloud federation during the establishment process. Hence, the load is dynamically adjusted to accommodate the static increase in workload as well as the dynamic changes in resources.

3.4.4.14. Standardization (Uniform access and management)

Considering that cloud federation integrates multiple cloud providers, standardizing interaction and communication as well as certifications are crucial and identified as a challenge in studies. Lack of global standards for interoperability of different cloud service providers, architecture, data access, data management, security, and other areas are the current major challenges. In addition, some of the challenges have been addressed by the studies, for example, resource allocation between cloud providers and data semantics to avoid duplication and corruption.

3.4.4.15. Optimal Resource Utilization

Optimal resource utilization measures the value of cloud resources in federations. With an effective strategy, it is imperative to optimize available resources. In some studies, this challenge is addressed by proposing strategies that identify unused or underutilized computing resources.

3.4.4.16. Availability and resilience

Availability and resilience of cloud federation is another challenge explored by studies, the availability of cloud federation is impacted by the availability of individual cloud provider resources

3.4.4.17. Optimal cloud federation formation

Another challenge identified is choosing the right cloud federation and making sure it is feasible for cloud providers. Considering the feasibility of cloud federation, especially the economic implications, the studies examine and propose a strategy for establishing an optimal and feasible cloud federation. Additionally, the cloud provider has to choose the right federation from the available group of cloud federations, and studies provide a mechanism for evaluating and selecting the most suitable coalition.

3.4.4.18. Market Competition and Cooperation

In cloud federation arrangements, various cloud service providers come together to work as one big service provider to overcome resource limitations and to have market control. However, it also comes with other challenges raised for this multi-tier dynamic market, in which cloud service providers not only cooperate with each other but also compete for consumers' requests. Establishing the healthiest cloud federation is another challenge addressed in the studies.

3.4.5. Existing Trends of Cloud Federation Formation

To answer the fourth research question (*RQ4: What are the latest research trends in the exploration of applied theories, methodologies, criteria influencing Cloud Federation Formation, evaluation metrics, and experimental environments utilized to measure the proposed solutions?*) in more detail, the information can be divided into five subsections. The first section summarizes the theories applied to establish cloud federation. The second subsection presents the proposed

solution (methodology) in general without delving into the details of the solution. The third and fourth sections present the factors influencing the cloud federation formation, followed by evaluation metrics utilized in the studies. In the last subsection, a description of the evaluation environment is described.

3.4.5.1. Applied Theories for Cloud Federation Formation

Establishing a cloud federation can greatly benefit cloud service providers and the intermediary cloud federation broker to overcome various limitations. In order for a cloud federation to be established, decision-makers must identify appropriate partners which have common objectives and meet the requirements. The outcome of this process determines whether or not the cloud federation will be established with the candidate cloud providers. Cloud federation partnerships are selected using various theoretical models that utilize a wide range of parameters. As shown in Figure 3.9, this review analyzed the existing literature. Game theory, Agent-based modeling, set theory, and numerical optimization theory are among the most commonly used theories in studies. Researchers have used existing theories and models to illustrate these facts, as shown in Figures 3.9 and 3.10.

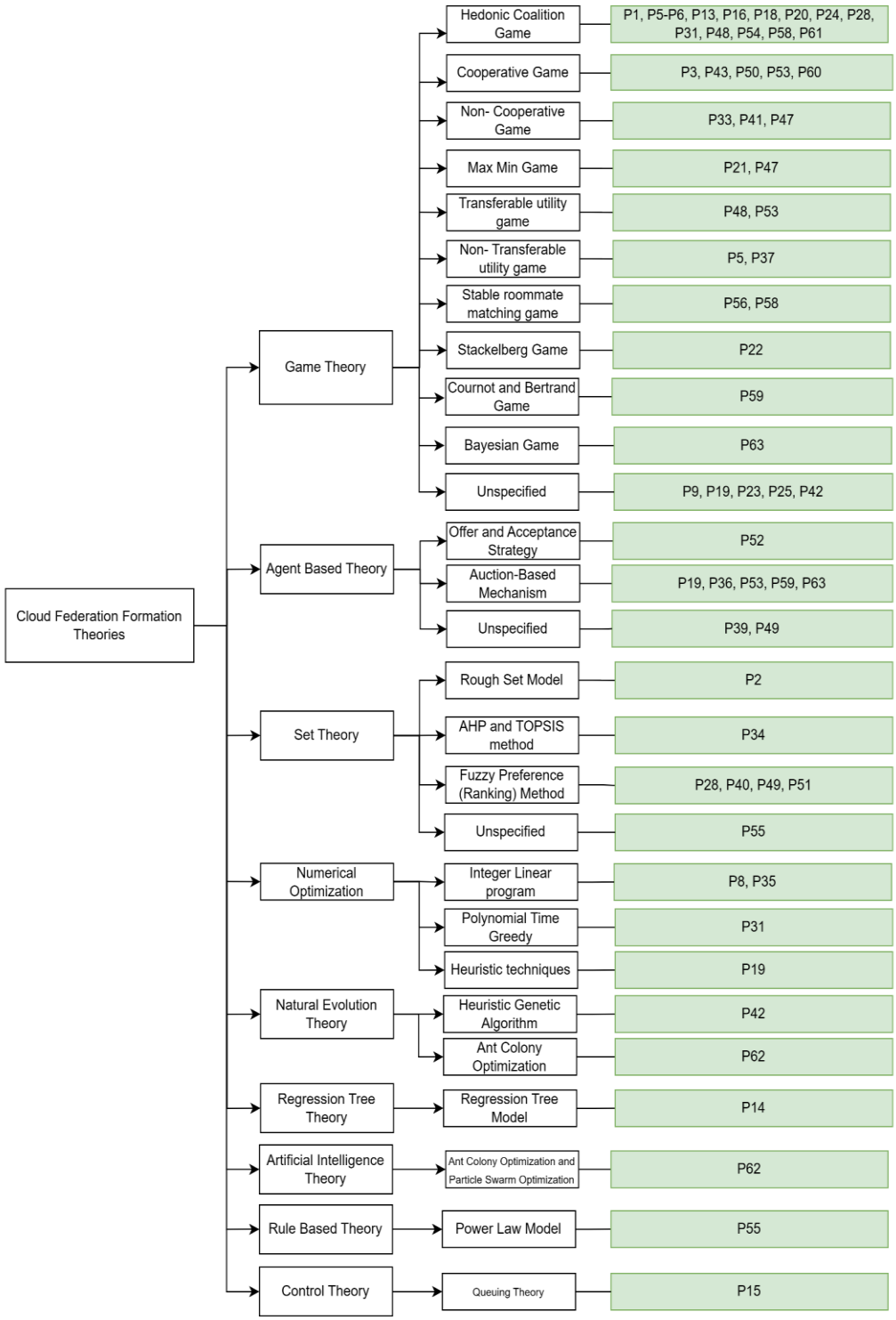


Figure 3.9: Theories adopted for cloud federation formation mapped with the studies (Appendix 1)

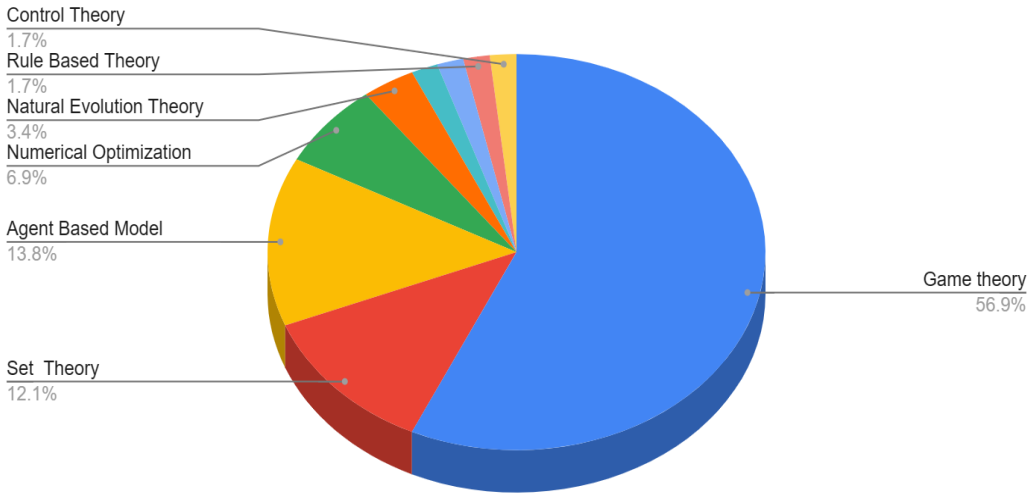


Figure 3.10: Theories adopted for cloud federation formation.

3.4.5.2. Proposed Solution for Establishing Cloud Federation

Following the existing study analysis, the proposed solutions for establishing cloud federation are divided into six categories: (i) Algorithms, (ii) Mathematical models, (iii) Frameworks, (iv) Architectures, (v) Policies, and (vi) Others. Many of the studies presented algorithmic solutions based on mathematical models. The algorithmic solutions are proposed for establishing the federation, while the mathematical model is proposed for calculating cloud service providers' behaviors so that the algorithm can determine whether to reject cooperation or establish it. Figure 3.11 illustrates cloud federation formation solutions and their categories. The result shows that 38% of the solution is algorithm-based and 44% is mathematical model-based.

Indeed, mathematical models, encompassing mathematical formulations and proofs, offer a means to determine and validate the selection of an optimal partner in cloud federation formation. The process involves proving or disproving the correctness of the cloud

federation formation algorithm based on specific specifications using mathematical techniques. Verification of these systems involves providing formal proof through an abstract mathematical model of the system. This correspondence between the mathematical model and the inherent nature of the system is ascertained by construction, ensuring the accuracy and reliability of the selected partner in the cloud federation. Mathematical methods thus play a crucial role in ensuring the soundness and effectiveness of the cloud federation formation process. The algorithmic solution on the other hand considers the key factors (functional and non-functional) influencing the cloud federation formation during the execution and establishment of cloud federation with the optimal providers.

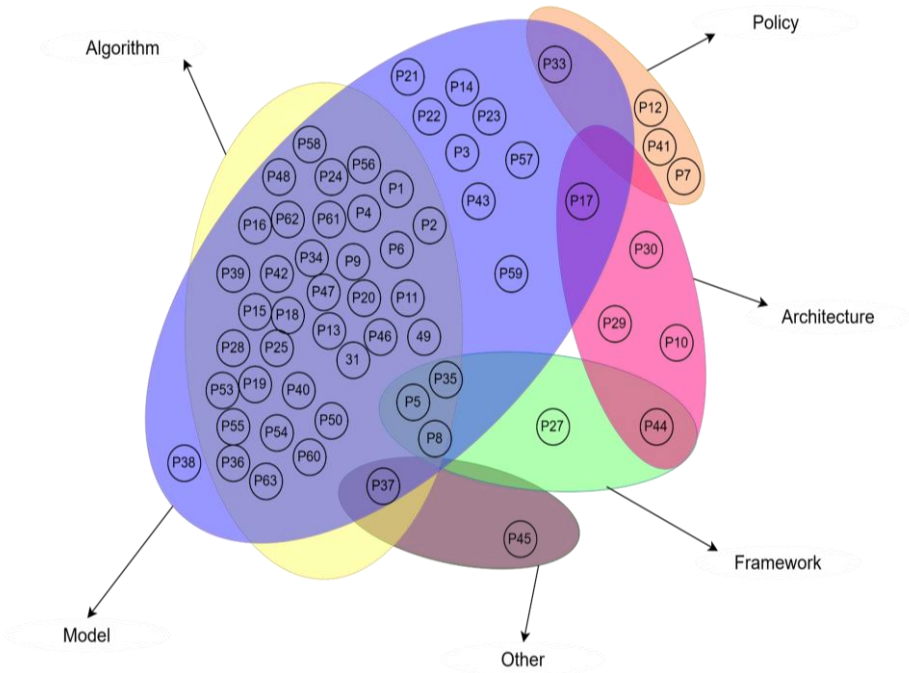


Figure 3. 11: Proposed solution of cloud federation formation

3.4.5.3. Criteria employed to Establish Cloud Federation

The selected studies investigate cloud service providers' behavior by examining the factors that influence cloud federation formation. As shown in figure 3.12, these factors are identified and summarized. Utility, cost, SLA (QoS) parameters, trust, security, resource information, and other factors influence the formation of cloud federations as presented in figure 3.12, and table 3.5. The widely explored factors to establish cloud federation are Resource information (such as the number of cloud service providers, Number of VM, the capacity of the resource, execution time, user workload, user resource request, and the like) and SLA (QoS) parameters (such as reliability, availability, scalability, responsiveness, KPI (uptime, downtime,...), QoS Parameters Indicator). The next widely utilized factor is costs like resource (VM) costs, operational costs, migration costs, energy consumption costs, and other related costs. Trust is another highly utilized influencing factor for cloud federation after cost parameters. Different trust factors are used to measure individual providers' trustworthiness and reliability. For example, recommendation-based trust utilizes neighbors' recommendations to calculate each cloud service provider's reputation and trustworthiness. Additionally, it can be policy-based trust that brings into play the cloud service provider's SLA parameters and reliability, or it can be evidence-based trust that considers the previous performance, feedback from the foreign cloud service provider, or feedback from the client. Cloud service providers' security parameters and utility are the next highly utilized factors, followed by other factors such as deadlines,

job schedules, or operating virtualization standards, which are considered as "other factors".

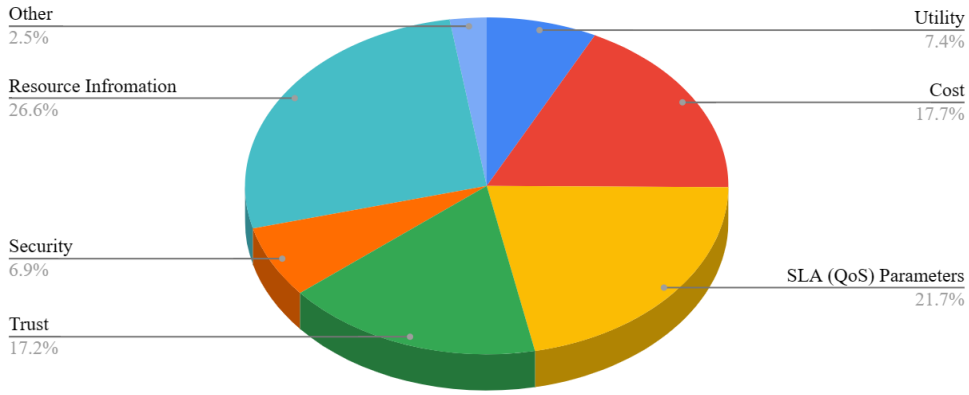


Figure 3. 12: The key criteria utilized for cloud federation formation

Table 3. 5: Details of key criteria used for the cloud federation formation

Key Factors	Details of the factors	Paper ID (Appendix 1)
Utility	Individual cloud service providers profit	P1, P8, P24, P25, P31, P33, P41, P50
	Satisfaction of the cloud service providers wrt QoS, Trust and/or profit	P15, P16 P21, P23, P49
	Expected profit	P33, P60
Cost	SLA parameters	P14, P15, P33, P34, P37, P41, P49, P52
	Migration cost	P19, P24, P34
	Energy consumption cost	P19, P22, P33, P41, P52
	Penalty Cost	P56
	Mislocalization Cost	P19, P58
	Operation Cost	P41, P53
	Mis-truthfulness cost	P58
	VM Cost (VM Price)	P8, P21, P22, P40, P42, P43, P48, P49, P50, P56, P58- P60, P63
SLA (QoS) parameters	Reliability	P8, P13, P17, P34, P38
	Availability	P8, P11, P13, P16, P27, P34
	Scalability	P8, P40
	Responsiveness	P13, P27, P34

	Redundancy	P38
	Competency	P17, P27
	Performance	P6, P8, P11
	KPI (uptime, downtime,...)	P27, P34
	QoS Parameters Indicator	P3, P6, P9, P11, P12, P14, P17, P18, P33, P35, P37, P39, P40, P41, P48, P52, P54, P57, P61, P63
Trust	Reputation	P4, P13, P39, P53, P55, P61
	Reliability	P17, P39, P55
	Previous Performance	P4, P5, P14, P20, P34
	SLA based trust	P4, P17, P18, P57
	Recommendation	P4, P5, P34, P50, P55
	Feedback based	P4, P14, P18, P39, P55, P57
	Other	P3, P16, P17, P51, P53
Security	Security standard and certification	P7, P10, P11, P30, P45
	Security risk level	P61
	Security Performance Parameter	P6, P11, P45, P51
	Security of individual cloud providers	P6, P7, P10, P14
Resource Information	Capacity of the resource	P25, P31, P36, P37, P56
	Number of cloud service provider	P17, P21, P25, P32, P42, P46, P47, P50, P53, P54, P55, P56, P58-P59, P62
	Number of VM	P21, P25, P42, P46, P48, P50, P54, P56, P58-P60, P62
	NIC address	P12
	Execution (Response) time	P2, P34
	User workload	P22, P31, P42, P47, P53, P54, P60, P62
	User resource requirement	P2, P35, P40, P54, P60
	Other	P5, P25, P32, P47, P58
Other	Deadline of the task	P2
	Job Schedule	P19
	Open Virtualization format standard	P12
	Externality Effect	P1
	Green tag of each server	P58

3.4.5.4. Evaluation Metrics

Cloud Federation formations studies utilized various evaluation parameters to evaluate and compare the proposed solution with the existing solution and show the performance. As the evaluation parameters are various and discussed differently, we summarized and categorized them into 8 evaluation groups: utility, processing time, quality of service, performance, cost, reliability, accuracy, and other evaluation. Figures 3.13 & 3.14 depicts the detailed classification of these evaluation metrics.

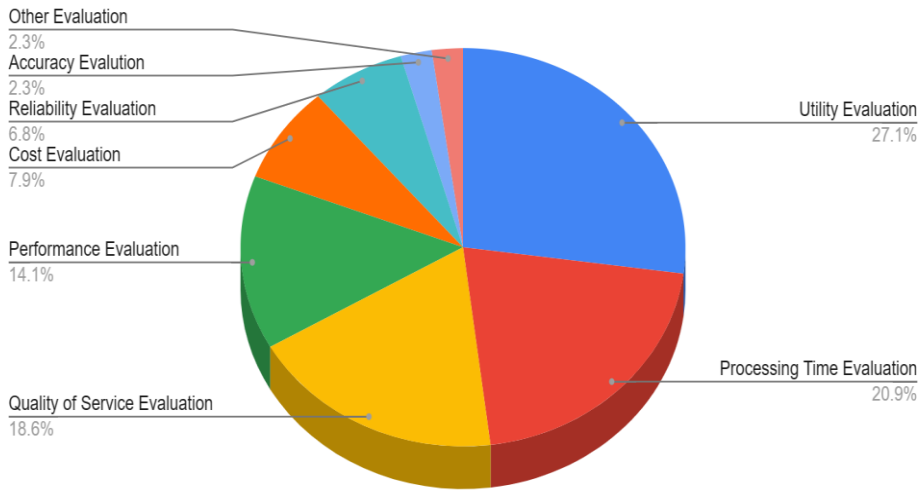


Figure 3. 13: cloud federation formation Evaluation Metrics

Utility Evaluation metrics are widely used to measure the satisfaction of cloud service providers and cloud federations. cloud service providers and cloud federation satisfaction levels are estimated by comparing their total (average) profits as well as the cloud service

providers of other members (Bouchareb & Zarour, 2021; Darzanos et al., 2019b; Dhole et al., 2016b; Hadjres et al., 2021, 2021; Hammoud et al., 2018b, 2020b; Hassan et al., 2016b; Khorasani et al., 2020; Moghaddam et al., 2020b; Nemati et al., 2019b; Ray et al., 2018, 2019, 2021b; Romero Coronado & Altmann, 2017b; Vadla et al., 2020b). Additionally, member satisfaction is affected by the average migration cost, since lower costs lead to more profit (Hammoud et al., 2020b; Ray et al., 2018, 2021b, p. 20), which in turn impacts their satisfaction, as well as their workload (high workload leads to high satisfaction)(Chen et al., 2017).

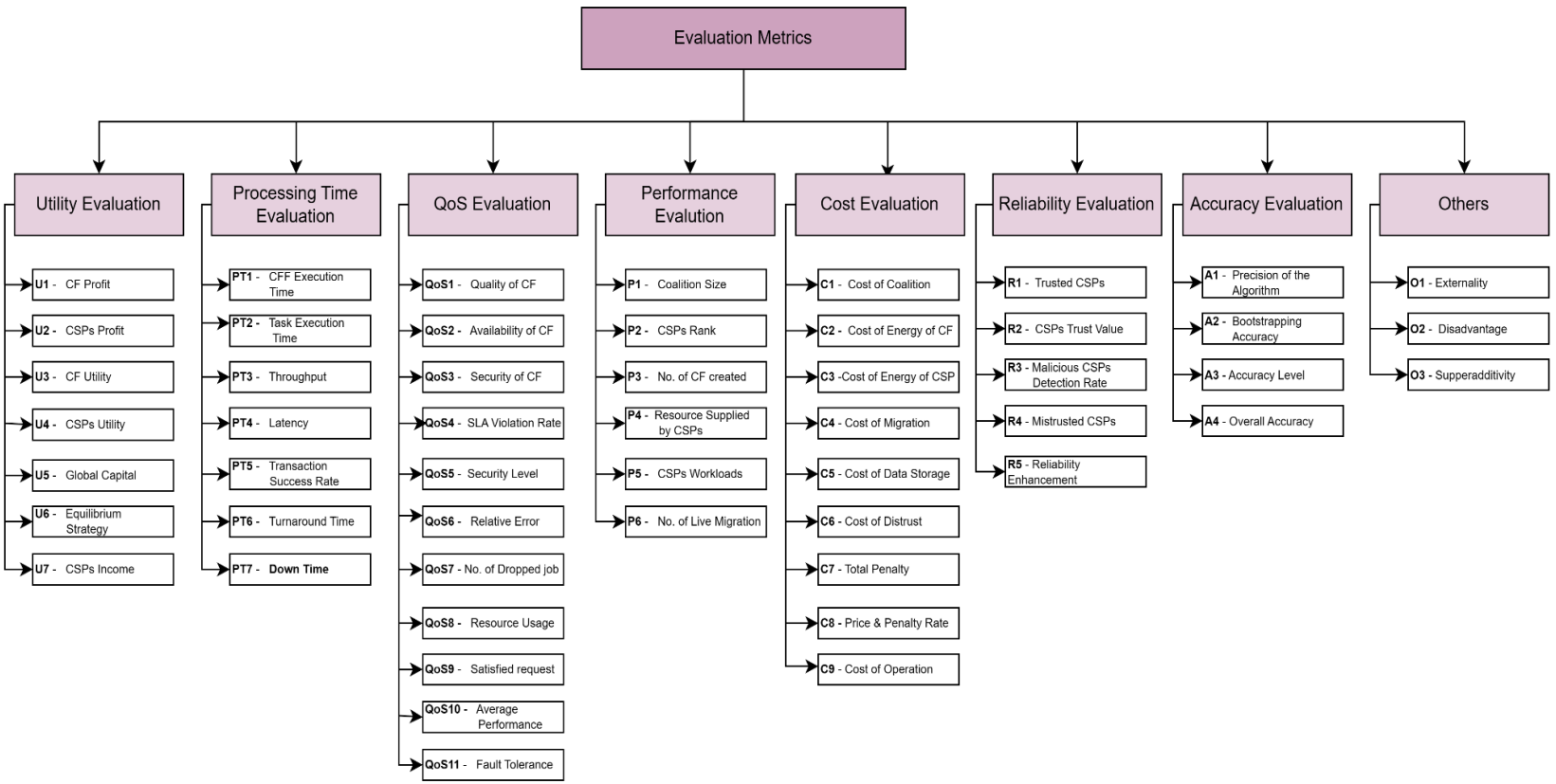


Figure 3. 14: Details of evaluation metrics (Refer Appendix A for mapping the articles)

Processing Time Evaluation includes cloud federation formation execution (response) time, task execution time, throughput, latency, transaction success rate, downtime, and turnaround time. Cloud federation formation execution time is a widely used processing time evaluation metric that focuses on formation runtime and the effectiveness of the proposed strategy. This is during an exhaustive search among a set of service providers to find the optimal federation partition. (Abusitta et al., 2018; Ahmed et al., 2021; Alam et al., 2020; Ayachi et al., 2021b; Barreto et al., 2021; Chen et al., 2017; Hadjres et al., 2020b, 2021; Halabi, 2018; Halabi & Bellaiche, 2020; Khandelwal et al., 2016b, 2018b; Mashayekhy et al., 2021b; Nemati et al., 2019b; Ray et al., 2019, 2021b; Satheesh & Aramudhan, 2019; Shi et al., 2022; Shrivastava & Pateriya, 2020b; Vadla et al., 2020b). The next highly utilized processing time metrics are tasks execution time and throughput to measure the number of requests that the coalition can handle in a given time (Abusitta et al., 2018; Fan et al., 2018; Gonzalez-Compean et al., 2018; Javed et al., 2020; K. Li, 2021; Maria Manuel Vianny & Aramudhan, 2017; Moreno-Vozmediano et al., 2017; Mourougan & Aramudhan, 2016b; Satheesh & Aramudhan, 2019; Wahab et al., 2018b; Najm & Tamarapalli, 2022).

Quality of Service Evaluation is the third most frequently used metric to evaluate the quality of established cloud federation. It provides

metrics regarding the quality of service in the established federation in terms of quality of cloud federation, availability of cloud federation, resource usage by cloud service provider, satisfied requests, average performance, fault tolerance, SLA violation rate, security of cloud federation, number of dropped jobs, and relative error (Abusitta et al., 2018; Ahmed et al., 2021; Biran & Dubow, 2019b; Comi et al., 2016b; Darzanos et al., 2016b, 2019b; Farris et al., 2017b; Gonzalez-Compean et al., 2018; Hammoud et al., 2018b, 2020b; Javed et al., 2020; Moreno-Vozmediano et al., 2017; Nemati et al., 2019b; Ray et al., 2018, 2019, 2021b; Shi et al., 2022; Wahab et al., 2018b).

Performance Evaluation is a metric used to evaluate the performance of an established cloud federation based on federation size, provider rank, number of cloud federations established, resources supplied by each member, and the number of live migrations. Specifically, the average number of cloud providers in a federation is widely utilized to predict a cloud federation's future performance.

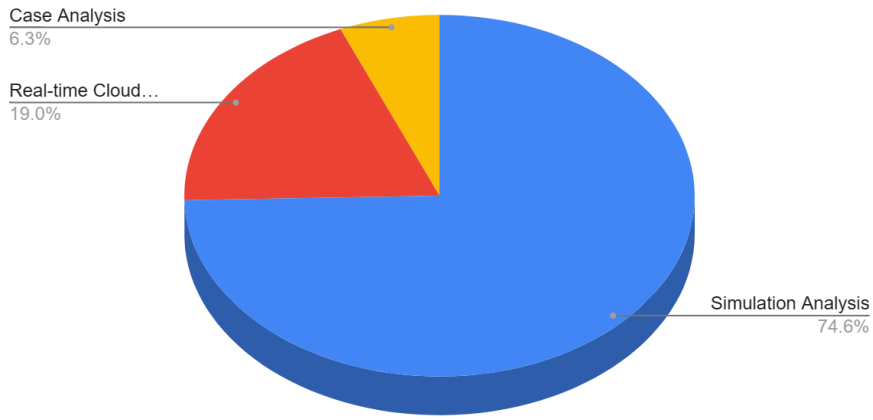
Cost Evaluation is a metric to depict the cost of the coalition, energy cost, migration cost, storage cost, cost of the district, penalty cost, and cost of operation.

Reliability evaluation is a metric to evaluate and distinguish the trusted cloud service providers, mistrusted cloud service providers, trust and reputation values of the member, and the malicious detection rate.

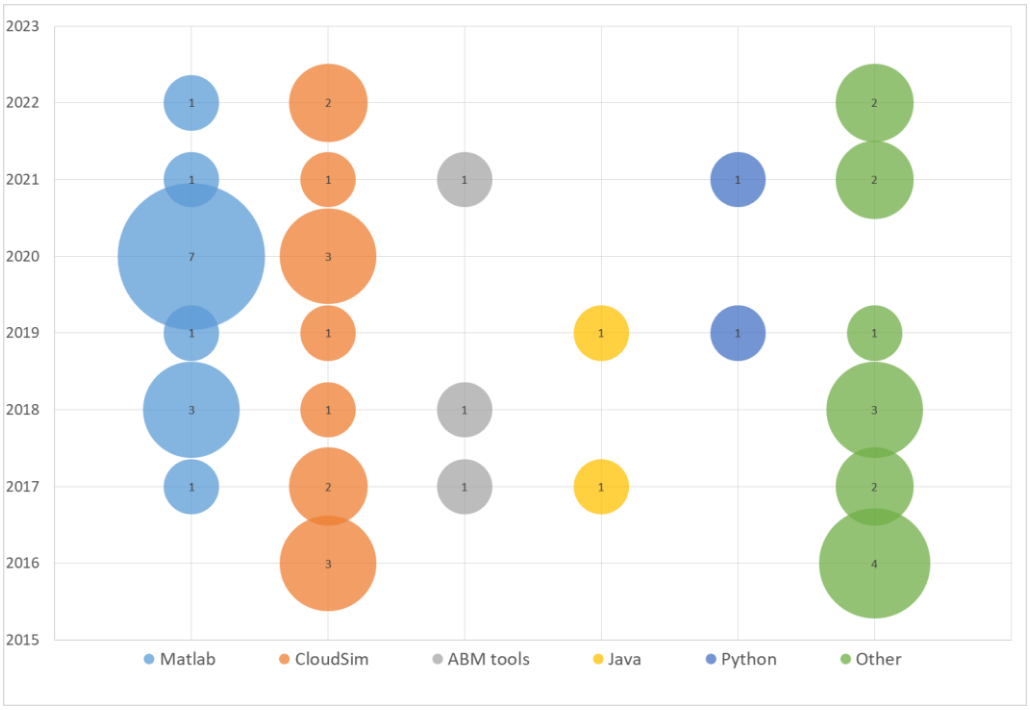
The last evaluation categories are ***accuracy level evaluation*** which depicts the accuracy and precision of a proposed solution, and ***other evaluations*** including externality, disadvantage, and supper additivity.

3.4.5.5. Evaluation (Experimentation) environment

Cloud federation formation experiments take into consideration the partner's dynamic behavior and current status; thus, it is practically difficult to experiment with cloud federation formation methods in a practical environment. Moreover, the cloud federation environment hasn’t been widely seen in the market except for some project initiatives. Therefore, evaluating the proposed techniques in a real-world cloud federation environment is even more difficult. As a result, most cloud federation evaluations have been performed using prominent simulation tools designed to analyze the proposed approach in the context of different real-world scenarios and to evaluate the performance of newly designed approaches. Figure 3.15 b) depicts that MATLAB and cloudSim simulation toolkits are the popular tools mostly used for cloud federation formation.



a)



b)

Figure 3. 15: a) Evaluation environments of the study b) Simulation tools used by the studies

3.5. Discussion and Implication of the Findings

This study focuses on the factors which are important to establish cloud federation. The study reviewed 63 journal and conference articles

on cloud federation formation. We designed four research questions to answer cloud federation enabling factors, requirements to establish cloud federation, current challenges, and current research trends such as applicable theories, proposed solutions, influencing factors, evaluation metrics, and experimentation environments. Based on the data extraction and analysis, 16 driving factors (section 3.4.2) and 17 requirements (section 3.4.3) are identified that can be used as a motive for establishing cloud federations and general requirements that should be considered. Additionally, 17 challenges (section 3.4.4) have been identified from the studies, including cloud federation stability and maximizing profit. A follow-up section discusses the current trends in cloud federation formation (see section 3.4.5).

Regarding applicable theories for cloud federation formation, game theory is identified as a widely applicable theory followed by set theory. In terms of the solutions offered, the majority of the current trends use algorithms with mathematical models to address cloud federation formation challenges. In addition, numerous studies use simulation environments to evaluate and compare the proposed methods. The most widely used simulation tools are MATLAB and the cloudSim simulation environment. The study also found that some experiments have been performed by creating real-time prototypes or using the cloud

computing environment to evaluate the proposed strategies. Appendix 1 summarizes the studies selected for this systematic literature review.

Table 3. 6: Summary of Findings and implications

Research Questions	**Findings**	**Implication**
RQ1	16 Enabling (driving) factors *(section 3.4.2)*	Knowledge-creation driven cloud federation is the least explored area
RQ2	17 requirements *(section 3.4.3)*	Formal institution requirements along with the Legal aspects and their effect on cloud federation hasn't been well explored
RQ3	17 challenges *(section 3.4.4)*	Maintaining the cloud federation stability in the presence of inter coalition conflicts need further study
RQ4	9 Applicable theories for cloud federation formation *(section 3.4.5.1)* 6 Kinds of Solutions *(section 3.4.5.2)* 7 Main Criteria to choose a partner *(section 3.4.5.3)* 8 Major Evaluation metrics *(section 3.4.5.4)*	The existing trend lacks distinguish between Vertical and horizontal cloud federation and address their issues accordingly. Experimenting with the proposed solution in a real-time cloud environment is the least explored.

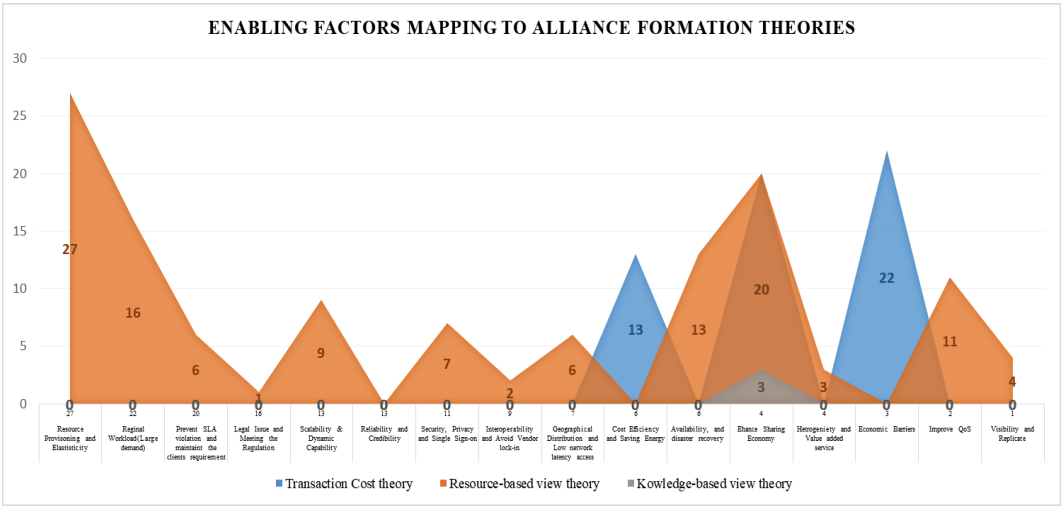
	3 Experimental Environments *(section 3.4.5.5)*	

3.5.1. Implications related to Cloud Federation Formation

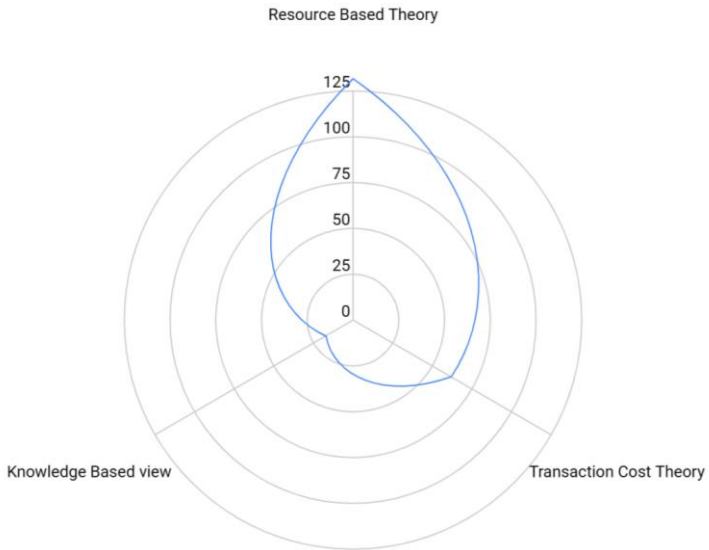
Enabling factors

In section 3.4.2, the cloud federation formation enabling factors have been explored. The analysis shows that the motives for establishing cloud federation are wide and deep and need to be observed from various perspectives. In order to analyze the enabling factors further, the strategic alliance formation theories are utilized due to the domain maturity level and the relationship between cloud federation and strategic alliances. Cloud federation is one of the technological alliances established between several cloud service providers.

Furthermore, analyzing these enabling factors with respect to alliance formation theory will show where the gap is and will give insight to fill the gap. Based on the use of these theories on the formation of technological strategic alliances, to understand their complexity from multiple theoretical perspectives, and a study by researchers in the relationship between these theories and different forms of technological alliance collaboration, the following three theories were selected. The theories are transaction cost economics, TCE (Williamson, 1975); resource-based view of the firm, RBV (Penrose, 1959); and knowledge-based theory, KBT (Grant, 1996).



a)



b)

Figure 3. 16: a) and b) show the distribution of the enabling factors w.r.t the strategic alliance formation theories

Most of the enabling factors examined in this study fit into transaction-cost and resource-based view theories, covering a broad range of theories. Nevertheless, the graph clearly indicates the lack of

studies in this area from a knowledge-based view theory perspective. Cloud federation establishes as task forwarding-based federation approach and capacity sharing-based federation approach. Especially in the late approach, it focuses on the capability of sharing either computing resources, data, or knowledge which could show that a knowledge-based view can be a foundational theory for establishing cloud federation and will show other cloud federation dimensions and applicability. Furthermore, the non-cooperative cloud federation is focused on maximizing their individual utility, but the cooperative cloud federation is focused on maximizing social welfare (Global Utility) and knowledge creation and sharing could be one of the objectives of creating a cooperative cloud federation. Therefore, **the knowledge-based view as a foundation theory for cloud federation formation should not be ignored and even need to be further explored to bursting knowledge creation-based cloud federation.**

3.5.2. Implication related to Cloud Federation Formation requirements

The previous studies in the cloud federation formation have focused on achieving a high level of trust to establish the federation or even establishing the trusted cloud federation with trusted cloud service providers. In 59% of the studies, the trust factors are based on the individual cloud providers' characteristics such as the provider's

reputation, a recommendation from the neighbor's cloud provider about the current providers, feedback from client or neighbor providers, and also the negotiation (SLA) parameters. By utilizing these factors, establishing trusted cloud service providers are the major objective trying to address many of the studies.

Trust is the home Cloud's expectation about the foreign Cloud's actions that affect the home cloud's choice to select the foreign Cloud for federation (and vice versa). After the trusted partner is selected, trust is still necessary to have a stable federation and continue with the collaboration as it is developed through the process. Trust development has several steps and levels of trust. At the partner selection stage, trust can be measured based on the trustee’s reputation or recommendation from neighbors' cloud service providers. During the agreement stage, the trust level between the trustor and the trustee can be evaluated by their agreement (SLA) terms and parameters. At the implementation stage, trust can be measured as how likely the partner cloud provider is to provide the requested resource to another cloud provider according to their SLA. Since trust is influenced by a variety of factors and is bidirectional, its development requires consideration of multiple factors and measurement at various stages.

According to the strategic alliance domain, trust does not depend on only the trustor and trustee’s characteristics, it also depends on other

external environments and their regulation. In addition, international trade studies justify that formal institutions (including laws, regulations, and rules that establish the basis for data ownership, data economy, and sharing) and informal institutions (including common values, cognitions, beliefs, traditions, customs, sanctions, trust and norms of behavior that are often expected or taken for granted) are significant factors, especially to the establishment of cross-border collaboration.

Cloud Federation is also a cross-border collaboration between cloud service providers, as resource elasticity and geographical distributions are some of the motives for cloud federation formation. Hence, formal institutions have a high impact on cloud federation effectiveness and stability. Regardless of this aspect, **the cloud federation formation studies lack addressing the formal institutions' requirement as one requirement to establish cloud federation**. Therefore, cloud providers should give attention to formal institutions as equal to informal institutions to establish cloud federation.

Moreover, the requirements (section 3.4.3) explored from the articles are general requirements for cloud federation formation that **require further research on the details of each requirement**.

3.5.3. Implication related to Cloud Federation Formation challenges

In the review study, it was found that the primary studies focused on cloud federation stability as their major challenge. Apart from being

the challenge, 36.50% of the studies tried to establish a stable cloud federation by employing various methodologies. Out of this 36.50%, 78.26% of them provide mathematical proof or prepositions and claim that applying the game theory, especially the Hedonic game theory establishes a stable coalition. However, 13% of them employ the Irving roommate algorithm with a strong justification that the algorithm creates a stable coalition. 4.3% of the studies try to address stability using the greed algorithm, and by evaluating the Jacobian matrix.

This further analysis shows that most of the studies addressed the stable coalition by providing mathematical proof of Nash stability and individual stability. Nash stability in cloud federations can be defined as the absence of an incentive for cloud providers within the federation to abandon their current federation. This is in favor of joining an alternative cloud federation.

Cloud federations, on the other hand, can be considered to be individually stable, if no cloud provider within the federation has the ability to gain from a move from its current coalition to a new coalition without adversely affecting the other members of that coalition in any way. 78.26% of the study raise the issue of stable coalition formation by utilizing a mathematical proof which is the manifestation of pure logic. However, it is necessary to verify these mathematical proofs according to the real-world scenario to be absolutely certain of the result. One of

the real-world scenarios is **and this and other scenarios need to be addressed in future works.**

3.5.4. Implication related to current trends

More than 56% of studies employ various kinds of game theory to establish cloud federations. As a result, game theory is one of the most effective theories of network formation, in which the optimal network is identified by analyzing players' opportunistic behavior. Leveraging game theory, practical scenarios such as pricing competitions and product launches, among other instances, can be systematically analyzed and forecasted for their potential outcomes. By applying game theory principles, real-world situations are modeled as strategic interactions between participants, allowing us to gain insights into the strategies they might employ and the subsequent results that could emerge. This approach enables us to anticipate and comprehend the dynamics of complex situations like pricing rivalries and product introductions, offering valuable insights for decision-making and strategy formulation in various competitive contexts.

Similarly, the studies employ game theory to identify the appropriate partners strategically utilizing various influencing factors. A horizontal cloud federation differs from a vertical federation, due to the different nature of the homogeneity and heterogeneity of the members. The study remains unclear about whether the existing networks are

horizontal cloud federations (SaaS-SaaS or PaaS-PaaS) or vertical cloud federations (IaaS-PaaS or PaaS-to-SaaS). **Vertical cloud federations have different forms and need to be addressed differently from horizontal cloud federations based on the same theory or any alternative theory that would be suitable for establishing them**.

With regards to the proposed solution and experimentation environment, 6.3% of the study used case analysis and the other 20.6% of the evaluation has been performed on the test bed cloud federation implemented at a small scale and in a real-world cloud computing environment. The rest 73% of the studies used a simulation environment to measure and evaluate the proposed solution. In some of this 73% of studies, very specific predictions are made regarding various aspects of cloud federation formation (see Figure 3.13). **Some of these predictions need to be tested in a real cloud computing environment or at least on the test bed by being directly exposed to data**.

Based on the stud findings, we point to the following interesting opportunities for future research:

1. Research on knowledge creation and knowledge sharing based cloud federation formation is required to expand the cloud federation application.
2. Further research is required to address the legal requirements during the partner selection stage.

3. Future research should focus on testing and verifying the proposed solution in real-world cloud federation environments.
4. Cloud Federation stability testing and verification need further investigation
5. In future studies, detailed requirements studies are required for each requirement specified in section 3.4.3, as the current study only considered the general requirements.
6. In order to gain a deeper understanding of cloud federation formation, this review can be complemented by looking at other research areas that incorporate principles from alliance formation, such as literature on partner selection for strategic alliances, and feature interaction that can also be seen as a way to manage alliance formation.

3.6. Conclusion

3.6.1. Summary

In this study, we perform a systematic literature review to study the key elements of cloud federation formation including the main enabling factors that lead to establishing cloud federation, major requirements, the current challenges addressed by the studies, and current research trends in terms of applied theories, types of solution provided, factors influencing the cloud federation formation, evaluation environment and evaluation metrics. Our focus was on research studies

reported in primary cloud federation journals and conferences. We aimed to answer four research questions by adopting the Okoli methodology and identified 63 primary articles which are relevant to answer the four research questions.

Research findings indicate that resource provisioning and flexibility are the most discussed enabling factors. Legal issues and meeting regulations, however, are the least explored enabling factors in the literature. There are 17 requirements for cloud federation formation, and trust and reputation among cloud service providers are the most explored requirements. This research also studies the challenges of cloud federation formation and has identified 18 major challenges. Among these challenges, cloud federation stability is the main issue discussed in the studies followed by Accounting, Billing, and Utility maximization issues. In the final section, we will analyze the current research trends in cloud federation formation in terms of applied theories, solutions proposed, factors influencing the cloud federation formation, evaluation metrics, and evaluation environment. Several kinds of game theory have been applied in the studies, followed by set theory. Most of the solution is proposed as a mathematical algorithm with extensive mathematical proofs, relying heavily on simulation environments to test and validate the solution. However, there are also a few papers utilizing the real-world cloud computing environment to test their solution. Moreover, the

factors influencing cloud federation formation are also explored along with evaluation metrics. Resource information and SLA parameters are the most common factors used in the proposed solution. The proposed solution was evaluated using metrics such as Utility, Quality of Service, and Processing Time.

The study's findings reveal that the discipline of cloud federation formation has evolved over time, introducing various solutions since 2016. However, despite the diversity of approaches, there is a common focus in their implementation. Many of these methods lack real-time evidence to substantiate the validity of their proposed solutions. To address this and enhance the appeal of studies to practitioners, we recommend the following:

1. Researchers should augment their studies by presenting more data and conducting experiments in real-world cloud computing environments. This will provide substantial support for their findings and persuade practitioners that their proposed solutions are indeed valid and practical.
2. To ensure clarity and comprehension among other researchers, detailed information about the research design, including elaboration on the credibility and robustness of the findings, should be provided. This transparency will facilitate better understanding and evaluation of the proposed approaches.

3. While algorithmic and mathematical models have their benefits, there is a need for more empirical experiments and industrial studies. Conducting such studies will not only optimize cloud federation formation rates but also cater to the specific needs and requirements of the computing industries. By combining theoretical models with practical real-world applications, researchers can provide more compelling evidence for the effectiveness and applicability of their approaches.

By addressing these points, researchers can strengthen the empirical basis of their studies and make them more appealing and relevant to both practitioners and the broader cloud computing community. Finally, the systematic literature review further presents implication and potential research directions with respect to these findings. Six recommendations that require further research are identified and presented in section 3.5.4.

3.6.2. Limitation

Our search was constrained to commence from 2016 onwards. This choice could impact the comprehensiveness of our search outcomes since our review does not encompass research published prior to the year 2016. However, as shown in section 3.2.2, there are some review studies published up to 2016. We tried to incorporate the findings of the review studies into this systematic literature review. Furthermore, this study

explores research from three databases (Scopus, Web of Science, and ScienceDirect). Similar work from another database is not taken into consideration in this study.

In addition, we found that some papers did not describe their approaches adequately or did not provide sufficient information to properly collect the data as described in the protocol. Therefore, we had to infer certain pieces of information during the data extraction process. To minimize the possibility of inaccuracy in the extracted data, the category is introduced through references to related studies and the recorded data as presented in the study.

Chapter 4. Institutional Quality Aware Trusted Cross-Border Cloud Federation Formation

4.1. Introduction

4.1.1. Motivation

Trust is a crucial factor in cloud federation formation, especially when it comes to the selection of cloud service providers to join a cloud federation. Selecting a trusted partner is essential for protecting customer data and ensuring that the cloud service providers perform according to the agreement, which ultimately results in social and economic benefits. cloud federation can be established within the country and across the country (AKA cross-border cloud federation). Cross-border cloud federations involve cloud service providers from different countries and require a different evaluation process for partner selection. This is because cross-border data flow is a sensitive issue and can be affected by various external factors such as the host country's political stability, the quality of their regulation, and so on.

The process of cloud federation formation involves the investigation and utilization of several criteria as cloud service provider assessment metrics, including trust, profit, performance, and strategic geographical position. Trust plays a pivotal role in the process of cloud federation formation and is described as the perception of the home cloud

regarding the behaviors of the foreign cloud. This perception significantly influences the decision of the home cloud in selecting the foreign cloud to establish a cloud federation. A trust evaluation across cloud service providers is a prerequisite and critical requirement to participate in a cloud federation and it varies depending on the trusted source and its evaluation model. Several trust sources have been explored, including the reputation of cloud service providers, feedback from users, and the SLA parameter.

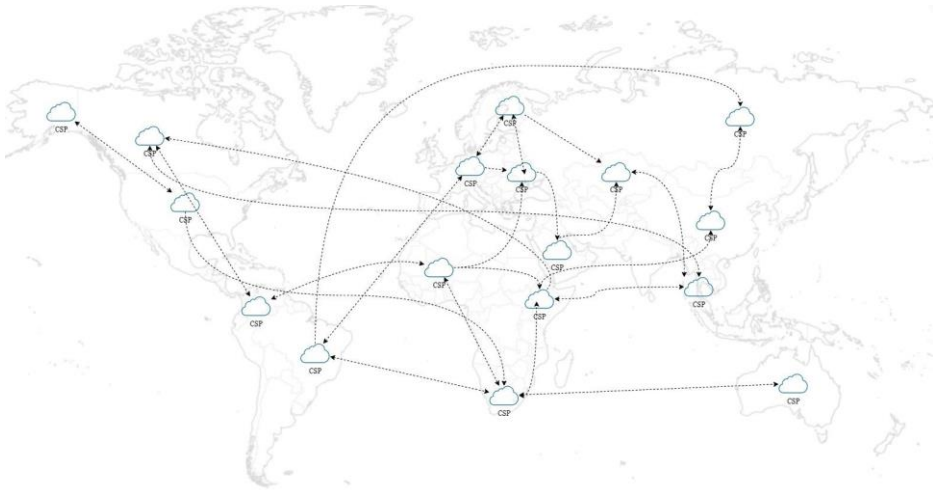


Figure 4.1 : Data Flow from one cloud service provider to another cloud service provider

Cross-border cloud federations have unique characteristics that must be considered during the partner selection stage. Host country status directly affects the business stability and protection of cloud federation. Moreover, data protection and privacy policy are also critical concerns related to the trust of the participants. The country's legal system, political relationship, regulation quality, and other concerns that

affect data flow, storage, and protection should be evaluated before cloud federation formation.

Overall, trust evaluation is an essential component of cloud federation formation, and this paper focuses on evaluating the trust levels between cloud service providers located in different countries by considering three trust sources, namely recommendations, Feedback, and the institutional quality index of the host country.

4.1.2. Relevance of study

In light of its potential to address key challenges associated with cloud computing, the formation of a cross-border trusted cloud federation deserves further research. Due to concerns over data security, privacy, and compliance with regulatory requirements, cloud service providers face a number of challenges. Having data stored in multiple jurisdictions can exacerbate these concerns, which makes ensuring compliance with data protection laws and regulations challenging. The institutional quality and reputation of a partner play a significant role in the evaluation of trust during the selection of cloud federation partners, in addition to the data protection measures considered as security measures. A cross-border trusted cloud federation that is institutional quality-aware can alleviate these concerns by serving as an early indicator of compatibility between cloud service providers by

considering institutional quality and reputation as one of the trust evaluation factors.

In addition, cloud computing has become an essential tool for businesses and organizations of all sizes, and the demand for cloud services is only expected to grow in the future. As the adoption of cloud computing continues to increase, the need for cross-border collaboration and cooperation between cloud service providers will become more important. In business, trust facilitates cross-border collaboration, and trusted cloud federations enable cloud service providers to work together more seamlessly and securely, benefiting both businesses and end users. Furthermore, the formation of a cross-border trusted cloud federation can help address the issue of market fragmentation in the cloud computing industry. Currently, the cloud computing industry is dominated by a few large players, which can limit competition and innovation. A trusted cloud federation that is open to multiple cloud service providers can provide a more competitive environment and foster innovation by enabling the exchange of data, applications, and services across different cloud platforms.

Therefore, institutional quality, which refers to the quality of the legal and regulatory framework within which cloud service providers operate, is essential to ensuring the success and sustainability of a cross-border trusted cloud federation and could give a guarantee for small-

scale providers to participate in the cloud federation. When cloud service providers are part of a trusted cloud federation, they can be assured that they are adhering to all legal and regulatory requirements and that their customers are receiving a high level of service quality. This can help build trust in the cloud computing industry and promote its growth and development. Hence, this paper is focused on evaluating trusted cross-border cloud federation formation considering the provider's institutional quality and presented the following sections accordingly.

This paper is divided into sub-sections. Section 2 presents the theoretical background and related works in the area. In Section 3, the methodology is presented in two parts, the first focusing on trust evaluation in forming trusted cloud federations and the second explaining how trust is calculated when incomplete information is available and there is evidence available. To demonstrate the trusted cloud federation formation visual effect, Section 4 presents the proposed experiment results using Netlogo simulation tools. After that, a Python implementation of a trusted cloud federation based on institutional quality is performed. Lastly, section 5 presents the discussion of the analysis and conclusion.

4.2. State-of-the-art

4.2.1. Trust Overview

Trust refers to the level of confidence that a cloud service provider has in another cloud service provider to securely and reliably provide and manage cloud resources on behalf of its customers (Ahmed et al., 2019).

4.2.1.1. Theory of Trust

Trust is a critical factor in enabling cloud federation, as cloud providers need to trust each other to work together effectively(Ahmed et al., 2019; Kanwal et al., 2014). To address this, a trust theory between cloud providers for cloud federation formation could be based on the following principles:

- Transparency: Transparency is essential in building trust between cloud providers (Ahmed et al., 2019, 2021). Cloud providers must provide clear and detailed information about their services, including their security policies, compliance certifications, and uptime guarantees. By providing this information, cloud providers can make informed decisions about which providers to partner with (Khan & Malluhi, 2010).
- Interoperability: Interoperability is essential in cloud federation formation, as it enables cloud providers to seamlessly work together (B. K. Ray et al., 2018b; Thomas & Chandrasekaran, 2017). Cloud providers must ensure their services are compatible

with other providers and that they use standardized protocols and APIs to facilitate integration (Khan & Malluhi, 2010; B. K. Ray et al., 2018a; Shrivastava & Pateriya, 2020).

- Security: Security is paramount in cloud federation formation. Cloud providers must implement robust security measures, such as encryption, firewalls, and access controls, to protect customer data and services from unauthorized access, theft, or misuse. Moreover, cloud providers must conduct regular security audits and assessments to ensure their systems are secure and up-to-date (Baldi et al., 2017; Bernabe et al., 2015; Chaimaa et al., 2017; Challagidad & Birje, 2020; Khan & Malluhi, 2010).
- Service-level agreements (SLAs): SLAs are critical in establishing trust between cloud providers. SLAs should define the availability, reliability, and performance guarantees of the services provided. SLAs should also include penalties for breaches, service credits, and dispute resolution procedures (Al Falasi et al., 2013, 2016; Chudasama et al., 2018; Vadla et al., 2020).
- Compliance: Cloud providers must comply with applicable laws and regulations, such as data protection, privacy, and intellectual property laws. They must also adhere to industry standards and best practices, such as ISO 27001, SOC 2, and NIST cybersecurity

framework(Massonet et al., 2011; Noltes, 2011; Singh & Sidhu, 2017)

- Contractual agreements: Contractual agreements are critical in establishing trust between cloud providers. Cloud providers must have clear and well-defined contracts that outline their responsibilities, obligations, and liabilities. Contracts should also address data ownership, data location, security and data portability to avoid conflicts and ensure customer data protection (Kertesz & Varadi, 2014; Nugraha & Martin, 2021).

4.2.1.2. Trust Dimensions

The article by Usma et al.(Ahmed et al., 2019) discusses the issue of trust in cross-cloud federation. According to the authors, trust in cloud federation has two dimensions: cloud consumer to cloud service provider trust, and cloud service provider to cloud service provider trust. However, depending on the cloud federation architecture, we identified the third dimension called cloud service provider-to-cloud federation trust.

The first dimension, cloud consumer-to-cloud service provider trust, refers to the trust established between the cloud consumer and the cloud service provider (Khorshed et al., 2011; Pearson & Benameur, 2010). This is a difficult task for consumers to measure, as they need to determine the trustworthiness of the cloud service provider from similar offerings. To evaluate the trustworthiness of the cloud service provider,

consumers can use a third party, such as a trust evaluator, who utilizes various factors such as the service level agreement (SLA), cloud service provider reputation, feedback from other consumers, and recommendation(Hosseinnezhad et al., 2021; Khan & Malluhi, 2010).

The second dimension, cloud service provider to cloud service provider trust, deals with the trust level of cloud service providers during provider-level cooperation (Ahmed et al., 2019, 2021; Bennani et al., 2014). Cloud service provider to cloud service provider trust is essential to ensure that the partner knows with what kind of provider they are dealing. The authors emphasize the importance of establishing trust between cloud service providers participating in the federation, as a breach of contract by one cloud service provider might have a domino impact on the performance of another participant cloud service provider, leading to customer mistrust.

The third dimension, cloud service provider to cloud federation trust, exists only if there is a mediator (cloud federation broker) between the service providers and consumers. As the cloud service provider and cloud federation brokers are different entities, trust between them affects the business process. The cloud federation requires cloud service providers to obey the fundamental code of conduct, disclose resource usage truthfully, and accurately uphold any signed SLA contracts. The authors suggest that in addition to utilizing the current trust evaluation

method from different sources, it is also important to consider the cloud service provider host country rules, regulations, and political stability to ensure the degree of data safety and accountability. This study is focused on evaluating the trust level between cloud service providers, with the goal of minimizing the risk of customer data protection and privacy issues.

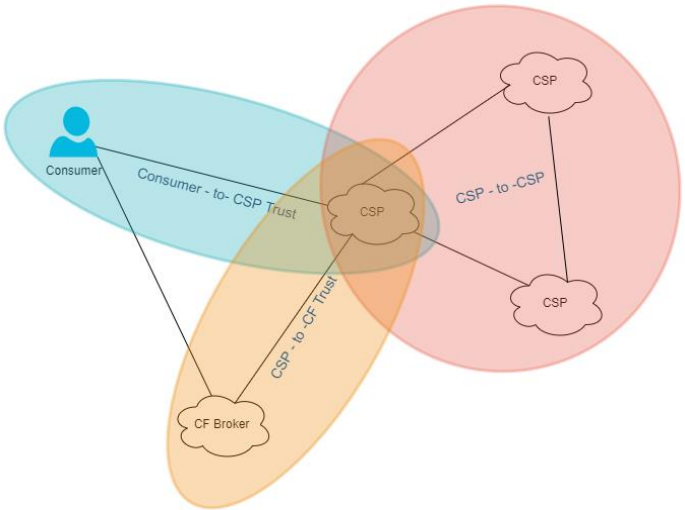


Figure 4.2: Trust Dimension (the figure is adapted from (Ahmed et al., 2020) with slight modification)

4.2.1.3. Trust in Cloud Federation

In recent years, several studies have proposed trust-based frameworks for cloud federation to address issues related to trust and resource management in a federated cloud environment. Mashayekhy et al. (2021) proposed a trust-aware inter-cloud resource management framework that considers both direct and indirect trust between cloud providers and covers the trustworthiness of both cloud providers and customers. (M. M. Hassan & Alsanad, 2016) presented a trust-based

resource allocation scheme that considers subjective trust mode and covers the trustworthiness of cloud providers. The proposed scheme enables cloud providers to establish trust and select appropriate partners for the federation. Wahab et al. (2018) proposed a trust-aware resource allocation framework that takes into account the subjective and objective trust modes and covers the trust level of cloud providers and their reputation in the federation. Dhole et al. (2016) presented a trust-based security framework that considers subjective trust mode and covers the trustworthiness of cloud providers. The proposed framework aims to enhance the security of data and resources in a federated cloud environment. Ahmed et al. (2021) proposed a trust-based virtual machine migration framework that considers both direct and indirect trust modes and covers the trustworthiness of cloud providers in the migration process.

Naseer et al. (2014) proposed a trust-based resource management framework that considers subjective trust mode and covers the trust level between cloud providers and customers in the federation. Ahmed et al. (2022) presented a trust-based dynamic resource allocation framework that considers both direct and indirect trust modes and covers the trust level of cloud providers in the federation and the demand for resources from customers. Ray et al. (2021a) proposed a trust-based service selection framework that considers both subjective and objective trust modes and covers the trustworthiness of cloud providers. The framework

enables cloud providers to select appropriate partners for federation based on their trust level. Halabi et al. (2018b) presented a trust-based security framework that considers both subjective and objective trust modes and covers the trustworthiness of cloud providers.

The proposed framework aims to enhance the security of data and resources in a federated cloud environment. (Hammoud et al., 2020)proposed a trust-based security framework that considers both subjective and objective trust modes and covers the trust level of cloud providers and their reputation in the federation. The framework aims to ensure the security of data and resources in a federated cloud environment. (Muralidharan & Anitha, 2022) proposes a Trusted Cloud Broker (TCB) system that evaluates the reputation of cloud providers in a federated cloud environment to assist users in selecting the most reliable and secure cloud services. The TCB system includes a reputation estimation model that considers multiple criteria, such as security, reliability, performance, and cost, and applies a fuzzy logic approach to calculate the reputation score of cloud providers.

In the studies, direct trust Quality and Profit Assured Trusted Cloud Federation Formation: Game Theory Based Approaches to the trust established between two parties based on their past experiences and interactions. In a cloud federation environment, direct trust between cloud providers can be established through past collaborations or successful

partnerships. Indirect trust, on the other hand, refers to the trust that is established through a trusted third party. For instance, if cloud provider A has established trust with cloud provider B, and cloud provider B has established trust with cloud provider C, then cloud provider A can indirectly trust cloud provider C through the transitive trust relationship between B and C. In this way, indirect trust can help establish trust between cloud providers who may not have had any direct interactions or experiences with each other. In the context of the studies mentioned, direct and indirect trust modes are used to establish trust between cloud providers and customers and to ensure secure and efficient resource management in a federated cloud environment. The studies propose various frameworks and schemes to address issues related to trust and resource management, utilizing subjective and objective trust modes, the trustworthiness of cloud providers and customers, trust level, reputation, and security.

Overall, the studies utilize various trust modes, including direct, indirect, subjective, and objective trust modes, and cover different dimensions of trust, such as the trustworthiness between cloud providers and their customers. Table 1 provides a summary of these studies.

4.2.1.4. Trust in Cross-Border Cloud Federation

In the context of the Cross-Border cloud federation, trust is a critical factor that impacts the success and stability of joint ventures (JVs)

between cloud service providers from different countries. Trusted cross-border cloud federation formation is a relatively the list explored topic, and as such, there is not a lot of previous research on this specific area. However, there has been some research on trust in cloud computing and cross-border collaborations that provide valuable insights into the topic.

In a study by Yan et al., (2023), the studies identified that institutional distance, which is measured by differences in institutional quality between a firm's home country and the host country, has a negative effect on trust between partners in the foreign market. This lack of trust can discourage firms from fully utilizing cross-border e-commerce platforms. The study suggests that this negative effect can be mitigated by pursuing faster internationalization strategies. This is because faster internationalization can help firms overcome the uncertainty and lack of trust associated with institutional distance, and build stronger relationships with partners in the foreign market. The report by (Vincenzo & Jan, 2020)finds that international agreements on cross-border data flows have a positive effect on the ability of firms to transfer data across borders. However, this effect is enhanced when there is a high level of institutional quality and standardization in the host country. Furthermore, the study highlights the important role of trust in building cross-border data transfer. The study finds that trust is positively associated with cross-border data transfer and that this relationship is stronger in the presence

of international agreements and high levels of institutional quality and standardization.

According to Lansing and Sunyaev, (2016) study, trust in cloud computing can be categorized into cognitive, affective, and behavioral trust. The study suggests that institutional quality plays a crucial role in building trust in any cross-border e-collaboration and that strong legal and regulatory frameworks can help to reduce perceived risk and uncertainty, ultimately enhancing trust between partners. The study underscores the significance of trust-building antecedents and institutional quality in building trust not only in cloud computing but also in cross-border e-collaboration. Another study by (X. Wang et al., 2015)focused on trust in cross-border e-commerce collaborations. The study found that institutional quality, cultural differences, and perceived risk were all factors that influenced trust in cross-border e-commerce collaborations. The authors suggested that building trust through institutional arrangements and communication could help mitigate the impact of cultural differences and perceived risk.

Overall, these studies provide valuable insights into trust-building strategies and factors that influence trust in cross-border collaborations. However, more research is needed specifically on the formation of a cross-border trusted cloud federation that is aware of institutional quality. This would help identify specific trust-building strategies and institutional

arrangements that could help mitigate the impact of cultural differences and institutional quality on trust in cross-border cloud federations.

4.2.2. Identification of Gaps and Problem Formulation

Several previous studies have explored the evaluation of trust in cloud computing and cloud federation by different researchers. As trust development is a process, the evaluation of trust differs in each cloud federation lifecycle. The evaluation of trust during partner selection or cloud federation formation is particularly important in enhancing and facilitating trust development in the remaining stages of the lifecycle.

Table 4.1: Related studies of trusted partner selection and applied game theory for cloud federation formation

Paper	Trust Dimension CF (Cloud Federation) CSP (Cloud Service Providers)	Trust Sources							Certainty of Trust	Used Approach
		Recommendation	Reputation	Feedback	Previous history	QoS and/or SLA Attribute	Security Attribute	Institutional Quality		
(Mashayekhy et al., 2021)	CSP - CSP	✓	✓	✓						
(B. Ray et al., 2018)	CSP - CSP					✓				
(Gupta & Annappa, 2016)	CSP - CSP	✓		✓	✓					
(Ahmed et al., 2022)	CSP - CF					✓				
(Abusitta et al., 2018)	CSP - CSP	✓			✓				✓	Dempster-Shafer
(Hassan et al., 2016)	CSP - CSP		✓		✓	✓				
(Wahab et al., 2018)	CSP - CSP	✓			✓				✓	Dempster-Shafer

(Dhole et al., 2016)	CSP - CSP	✓			✓					
(Ahmed, Raza, et al., 2021)	CSP - CSP	✓				✓	✓			
(Naseer et al., 2014)	CU - CSP					✓				
(Ray et al., 2021a)	CSP - CSP					✓				
(Halabi et al., 2018b)	CSP - CF						✓			
(Hammoud et al., 2020)	CSP-CF		✓		✓					
(Papadakis-Vlachopapadopoulos et al., 2019)	CSP-CSP		✓			✓				
This Study	CSP - CSP	✓ (Eq. 2)	✓ (Eq. 2)	✓ (Eq. 11)	✓ (Eq. 7)	✓ (Eq. 6)		✓ (Eq. 4)	✓ (Eq. 3, 14, 15, 16, 17, 18)	Heuristic Approach

Table 4.2: Related studies of applied game theory for cloud federation formation (N/A stand for Not Applicable)

Paper	Game Theory Type	Similarity	Difference
(Mashayekhy et al., 2021)	Cooperative Coalitional Graph Game (with Transferable Utility)	Individual Stability Transferable Utility	• Trust evaluation model(Global trust is calculated first) • Source of Trust • Graph Theory is incorporated
(B. Ray et al., 2018)	Hedonic Coalition game	N/A	N/A
(Gupta & Annappa, 2016)	Non-Game Theory	N/A	N/A
(Ahmed et al., 2022)	Non-Game Theory	N/A	N/A
(Abusitta et al., 2018)	Hedonic Coalition game	N/A	N/A
(Hassan et al., 2016)	Cooperative Coalition Game (with Transferable Utility)	Individual Stability Transferable Utility	• The broker announced the price rate with require resource • Source of Trust • Different Trust Evaluation
(Wahab et al., 2018)	Hedonic Coalition game	N/A	N/A
(Dhole et al., 2016)	Cooperative Coalition Game Theory	Trusted coordinator	• The coordinator Announce maximum selling price. • The number of required resource thresholds is set

			by the coordinator ● The coordinator calculated the trust of cloud service providers
(Ahmed et al., 2021)	Non-Game Theory	N/A	N/A
(Naseer et al., 2014)	Non-Game Theory	N/A	N/A
(Ray et al., 2021a)	Hedonic Coalition game (with non-transferable utility)	N/A	N/A
(Halabi et al., 2018b)	Hedonic Coalition game	N/A	N/A
(Hammoud et al., 2020)	Non-Game Theory	N/A	N/A
(Papadakis-Vlachopapadopoulos et al., 2019)	Non-Game Theory	N/A	N/A
This Study	Cooperative Coalition Game (with Transferable Utility)	Trusted coordinator Individual Stability Transferable Utility	● Trust Source ● The coordinator provides recommendation/ feedback information ● Each cloud service provider evaluate their trust towards other cloud service provider (Distributed trust evaluation) ● Individual cloud service provider announce their price and the requester announce the required resource and it's WTP

Therefore, it is crucial to ensure that the trust evaluation in the cloud federation stage is certain, reliable, and accurate, particularly when limited information is available or when the trust source reliability is unknown. The research on trust evaluation for cloud federation formation, is summarized and presented in Table 4.1 and identified the literature gap.

- Trust evaluation in cloud computing can be challenging, particularly when limited information and subjective measurements are used. Subjective measurements, such as reputation or recommendation from other cloud service providers, can be influenced by personal biases and preferences, which may not accurately reflect the true trustworthiness of a service provider. When the number of subjective measurements is limited, the trustworthiness of a service provider may be compromised due to the small number of opinions given, and the potential for personal interests to influence those opinions. Therefore, there is a need to incorporate other trust sources, such as a generalized objective measure, which can be computed from institutional quality. Institutional quality provides information about the external environment of cloud providers, including their legal system, regulatory quality, and cultural context, which is significant in assessing trustworthiness. Furthermore, the

evidence from the previous literature shows (section 4.2.1.4) the importance of incorporating institutional trust with other trust sources to determine the effect of the institutional trust computed from institutional quality especially to compute trust. Therefore to understand the effect of institutional trust on the overall trust computation and cloud federation formation, we design the following research questions.

RQ2-1. How does incorporating institutional trust impact the overall trust evaluation process and consequently influence decision-making for cloud federation formations?

This research question aims to explore the impact of institutional trust on the overall trust evaluation process and its role in decision-making for cloud federation formation. It emphasizes the examination of both formal and informal institutional trust. To evaluate informal institutional trust, the study incorporates recommendations from peer providers, which serve as a subjective measure. This enables the computation of informal institutional trust by considering the opinions and experiences shared by peers. On the other hand, for formal institutional trust, the study utilizes institutional quality parameters obtained from the world governance data. These parameters are employed to calculate the formal institutional trust, providing a quantitative

assessment of trust within formal institutional frameworks. By incorporating these approaches, the study aims to comprehensively assess the impact of formal and informal institutional trust on the overall trust evaluation process and cloud federation formation.

- Trust development is a gradual process, and it is important to continuously work towards maintaining that trust in the future. One of the processes of forming a trusted cloud federation after the interaction is using feedback collected from users and/or peer providers. While feedback is an essential tool for evaluating the performance of cloud providers, it is often subjected to bias and exaggeration. The problem statement is that the feedback collected from users and/or peer providers during the process of forming a trusted cloud federation may not always be reliable and accurate. In fact, one of the current issues in small-scale providers is fake review attacks (Negative feedback attacks or Bad-mouthing attack) which have a big impact on small service providers. This can be due to a variety of factors, such as the subjectivity of user feedback or the tendency of peer providers to exaggerate their own capabilities, to dragging down the reputation of small-scale providers' dues to conflict of interest and the like. As a result, the evaluation of cloud providers' trust

based on feedback can be unfair, and inaccurate, leading to the formation of less reliable and less trustworthy cloud federations. Therefore determining the exaggerated outlier feedback is important for reliable and accurate trust evaluation. Several studies tried to address such issues by using the Bayesian inference or Dempster-Shafer theory. This approach is suitable when the evidence is accurate and reliable. However, when it comes to the false feedback attack or bad-mouthing attack, several cloud service providers can cooperate to provide negative feedback and the trust computation using these two approaches can be affected and the result could be inaccurate or unreliable since these techniques. Therefore, addressing the trust accuracy by addressing the feedback credibility that affects small-scale providers are significant to allowing fair and inclusive cloud federation formation.

RQ2-2. How does we ensure the accuracy of trust calibration in cloud federation formation when feedback collected from users and/or peer providers is subject to bias and exaggeration, including false feedback attacks?

This research question aims to explore the way to identify malicious feedback from users and/or peer providers to compute trust aggregation.

4.3. Proposed Trusted Cloud Federation Formation Model

We propose an IQ-aware trusted cloud federation formation in light of the current research gaps in this field. Cloud federations combine multiple cloud service providers, cloud devices, fog nodes, and edge devices to provide a service to customers. For this reason, the cloud federation needs to be established between the trusted cloud service providers to determine the right trusted device to allocate the tasks. The providers will allocate tasks based on the customer's preference for a reliable and trustworthy cloud service provider. The task will be assigned by considering the information regarding the member cloud service providers in coordination with service providers. This information can be used to compute and determine the reliability and trustworthiness of cloud service providers. Then the task will be signed to the trusted provider with maximizing the utility of the requester provider.

4.3.1. Architectural Overview and overall process (System Architecture)

The architecture shows a trusted coordination system that involves a coordination service provider (Coor), multiple cloud service providers, Smart contracts, databases, and a trust evaluation model. *Coordination Service Provider (Coor)* is a trusted entity that provides a coordination service for various devices and cloud service providers. The coordination service includes keeping a registry of all registered devices

in each cloud service provider, running a database for device ratings by other cloud service providers and customers, ranking about data handling policies of countries, and ranking about privacy regulation of countries. The Coor also analyzes and updates information about cloud service providers and their services. *Cloud service providers* are companies that provide cloud computing services, such as storage, networking, and computing power. The cloud service providers register with Coor and provide such as name, location, and services offered, by providing a smart contract. *Smart Contracts* are self-executing contracts with the terms of the agreement between the cloud service provider and the Coor, which are automatically enforced via software code. *Database*: Coor runs a database that stores all the registered devices and cloud service providers, as well as all device ratings, ranking about data handling policies of countries, and ranking about privacy regulation of countries. This database is used to fetch information about other cloud service providers' ratings and ranks when a cloud service provider initiates a request to Coor. *Trust Evaluation Model* is a model that the cloud service provider utilizes to determine the trustworthiness of other cloud service providers and rank them according to their trust level.

In Figure 4.3, the overall interaction steps are presented. The first step in the interaction is the registration of the cloud service providers with Coor, providing their basic information and services offered by

providing a smart contract. Coor then collects more information about the cloud service providers from various sources such as public databases, customer reviews, and performance metrics. The collected data is then analyzed, and the rating of all the devices, ranking about data handling policies of countries, and ranking about privacy regulations of the country are stored for future use. When a cloud customer resource request is made, the cloud service provider initiates a request to Coor for information about another cloud service provider's rates and ranks. Coor validates the request to ensure that it is coming from an authorized cloud service provider. If the rating data is not available, the Coor provides the recommendation data regarding the cloud service providers that are collected from other member cloud service provider opinions. Coor fetches the rating and ranking information about the requested cloud service provider from its database and signs a smart contract with the requesting cloud service provider before sharing the information. The contract specifies that the requesting cloud service provider will not disclose the provided information to third parties.

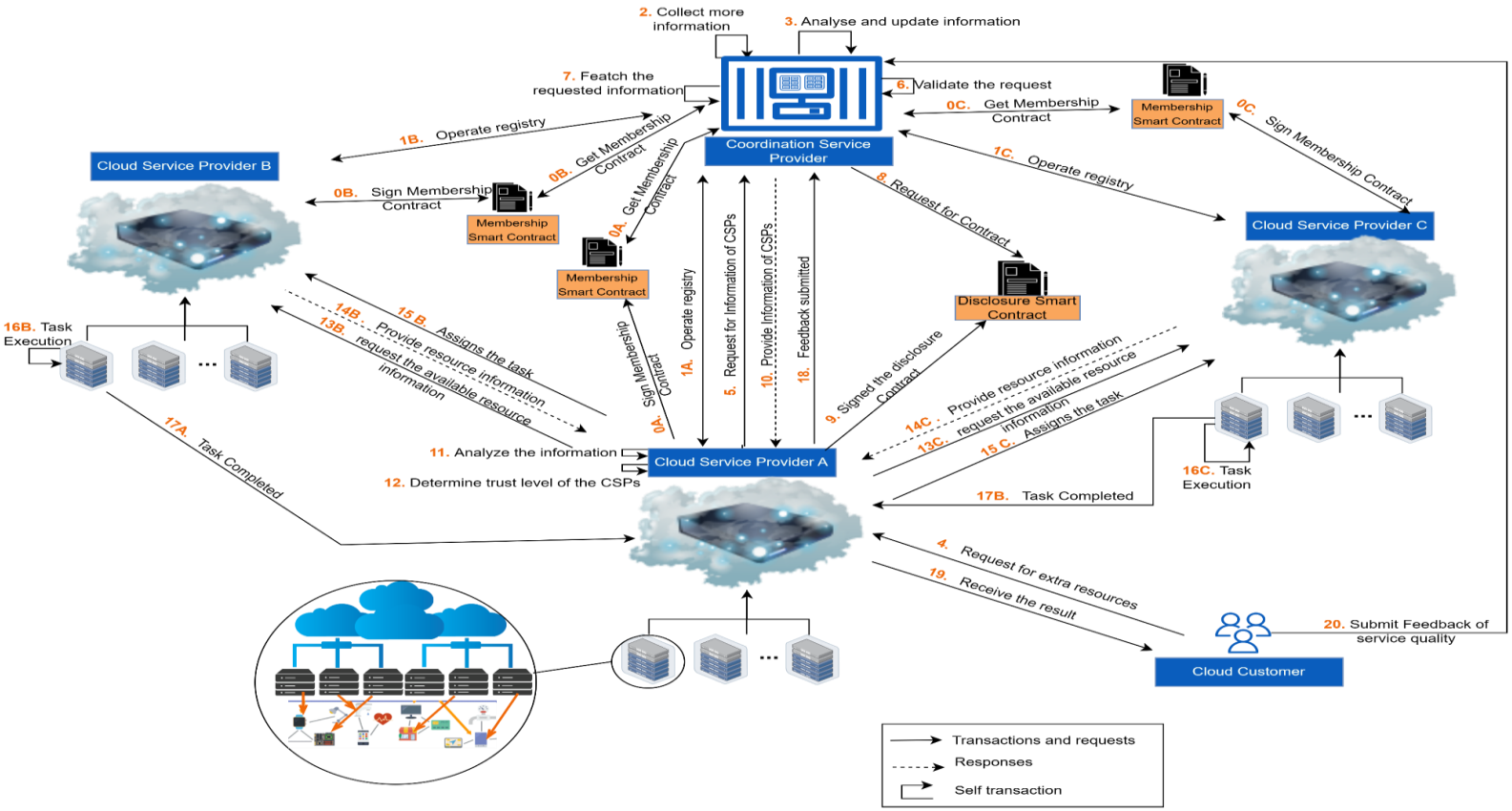


Figure 4. 3: The interaction of the components

The requesting cloud service provider then analyzes the provided rating and ranking level information to determine the trustworthiness of the cloud service providers whose information was requested. Based on the analysis, the requester will get the list of potential partners with their trust level above the required threshold. The potential partner cloud service providers receive the request for their available resource information and unit price. Then after the requester cloud service provider chooses the cloud service provider with the lower price offer from the potential partner lists and assigns the task to that cloud service provider. If the first selected cloud service provider from a potential partner has enough available resources, it assigns the task to a single cloud service provider. Otherwise, the cloud service provider from the partner list that offers the second lowest price will be assigned the rest of the tasks. After the task completion, the requesting cloud service provider verifies the completion of the task and provides feedback to the partner cloud service providers. The requesting cloud service provider also provides feedback to Coor regarding the service quality of high-trust cloud service provider task execution. Coor collects more feedback from the user and updates the information of high-trust cloud service provider for the next (future) use.

The overall architecture is supported by a coordination service provider that provides a registry, runs a database for device ratings, and

keeps rankings of data handling policies and privacy regulations of countries. The system is designed to be fully distributed, and the decision about trusting the cloud service providers lies only with other cloud service provider that require extra resources.

4.3.2. Institutional Quality Aware-Trust-based Cloud Federation Formation

The cloud federation formation is initiated by the cloud service provider when the extra resource request from the cloud customer is received. At this stage, the cloud service provider interacts with the Coor and a potential partner cloud service provider to get the necessary information that will guide to computing trust level and establish a coalition that will maximize the requester cloud service provider utilities. To do so, a game theory approach is utilized to analyze the behavior of decision-makers in strategic situations. It is possible to consider cloud federation formation among cloud service providers as a strategic situation where several self-interested parties come together to form an alliance or group to accomplish a common objective. In a cloud service provider setting, cloud federation formation can be modeled and analyzed based on game theory. This is because it provides a formal and rigorous framework for studying the interactions between individual cloud service providers who have self-interests in maximizing their utilities. Specifically, game theory enables cloud service providers to

model the incentives and constraints that they face when deciding whether to form a coalition. Moreover, it provides a method of allocating resources and distributing the coalition's benefits and costs.

4.3.2.1. Game Formulations and Assumptions

A coalitional game is a method rooted in game theory that provides a framework for modeling interactions among multiple players as they make decisions about cooperating through group formation. The result of this game entails a definitive partitioning of coalitions across the set of players. In our cloud federation formation, the players in the game are individual cloud service providers and the caption to be formed are called cloud federation. The objective of the providers is to form a trusted cloud federation based on the cloud customer and requester cloud service provider's trust preference to address the resource scarcity of each cloud provider by renting idle resources from their partner providers. In this study, a cooperative coalition formation game with a transferable utility is employed for the cloud federation formation. Cooperative game theory is often used for coalition formation in situations where multiple players can benefit by working together towards common objectives or goals.

Property 1. *The proposed game is a cooperative coalition formation game.*

The objective of this study is to form a trusted cloud federation in which the number of untrusted cloud service providers is minimized, equal chance is provided for small-scale cloud service providers and large-scale cloud service providers to be the coalition members, and established the core coalition for the requester to maximize the requester utilities and increase the stability of the coalition. Therefore the objective of this paper is to establish the core coalition with the trusted cloud service providers depending on the requester cloud service provider characteristics and preference on the way trust is evaluated considering a fair environment.

The proposed game involves cloud service providers acting as players and aims to establish coalitions known as Cloud federations. In this context, cloud service providers seek to join federations that consist of desirable members based on trust. Each provider acts in its self-interest when deciding which federation to prefer over others. To elaborate further, we formally define the concept of federation formation from the perspective of coalitional games. The cloud federation game is introduced as a cooperative coalitional game, which examines interactions between groups of decision-makers (i.e., players). Within coalitional games, players have the ability to collaborate and form alliances while striving to maximize their utility. Consequently, we define the cloud federation game as a specific type of coalitional game

with transferable utility. This means that the value or utility generated by a coalition can be divided and shared among its members in a meaningful way, enabling players to negotiate and make decisions about joining federations based on the expected benefits they would receive. We define a cloud federation game as a coalitional game with transferable utility as follows:

> **Definition 1.** (Ayachi et al., 2021)" *A coalition is a set of players that seek to form cooperative groups in order to strengthen their positions in a game. Any coalition* $S \subseteq N$ *(*N*: set of players) represents an agreement between the players in* S *to act as a single entity. In case* $S = N$*, we speak about a grand coalition.If* $|S| = 1$*,* S *is called a singleton or trivial coalition".*
>
> **Definition 2.** (Ayachi et al., 2021) *"A cooperative game is defined by a pair* (N, v) *where:*
>
> - $N = \{1, \ldots, N\}$ *set of players*
> - v*: a function that quantifies a coalition value in the game. If the coalition value depends only on its members, then the game is in characteristic form".*

Property 2. *In the proposed cooperative coalition game the cloud service providers are individually rational.*

The proposed cooperative coalition game satisfies individual rationality, meaning that each cloud service provider has a dominant

strategy to participate in the coalition that results in a non-negative utility for themselves, regardless of the strategies chosen by the other cloud service providers. Every cloud service provider will only join the coalition if they expect to gain at least as much utility from it as they would by not joining the coalition. As a result, each cloud service provider will be able to have a positive utility in the game as a result of participating in the coalition, which means that they will not be worse off than they would be if they did not take part in the coalition.

Property 3. *The proposed cooperative coalition game is a transferable utility (TU) game.*

The total payoff of the coalition can be divided among its members in any way that they agree upon. In a transferable utility game, the value or utility that each player receives from the coalition is transferable or divisible. This means that each player's contribution to the coalition's total value can be measured and divided among the players in any way that they agree upon. In the context of cloud federation formation, this implies that the benefits or payoffs that the coalition generates, such as profit or global trust, can be divided among its members in a way that reflects their respective contributions.

> **Definition 3** (Petri, Rana, et al., 2015) *"A coalitional game with Atransferable utility is a pair* (N, v)*, where* N *is the set of players and* v *is defined as":*

$v : 2^N \rightarrow \Re^{|S|}$ *is the characteristic functions.*

For each $S \subseteq N, v(S)$ *is the value that the agents can share amongst themselves.*

$$v(\phi) = 0$$

A transferable utility game is a cooperative game in which the players (cloud service providers) can form coalitions and share the benefits (utility) of being in the coalition. The utility can be seen as the trust level that each cloud service provider can contribute to the coalition. The utility is transferable because the coalition members can redistribute the benefits among themselves according to some rules. The trust levels and the coalition profit in this study are seen as the utility that each cloud service provider can bring to the coalition, and they can be transferred between the coalition members. The goal is to form coalitions that maximize the overall trust level of the coalition and the utility of each cloud service provider.

Property 4. *The proposed cooperative coalition game is a core of TU game for the requester cloud service provider.*

The core coalition refers to a group of cloud service providers that have formed a stable coalition with the requester cloud service provider. The coalition is self-enforcing because it is in the best interest of each member to continue cooperating with the others. It is possible that a core coalition can be established for the requester cloud service

provider in this game. The rules of the game and the distribution of resources determine whether such a core coalition is possible. In this case, the core coalition would consist of the cloud service providers that have formed a stable and self-enforcing coalition with the requester cloud service provider, and it would be in the best interest of each member to continue cooperating with the others.

Definition 4 (Petri, Rana, et al., 2015) *"The core of a TU game (N, v) is the set of all payoff allocations that are individually rational, coalitional rational, and collectively rational. In other words, the core is the set of all imputations that are coalitional rational". Thus we have*

$$Core\ (N,v)\ =\ \{(x_1,\ldots,x_n)\ \in\ R^n\colon \sum_{i=1}^{n}\ x_i\ =$$

$$v(N);\ \ \sum_{i=C}\ x_i \geq v(C)\ \forall C \subseteq N$$

A coalition C can be improved on an allocation of

$$x\ =(x_1,\ldots,x_n)\ \in\ mathbbR^n\ iff$$

$$v(C)\ >\sum_{i=C}\ x_i$$

Definition 5 (Guosun et al., 2022) "*(User Tasks) a user task is a user service whose request is submitted to the federated cloud computing platform and can be executed by any of the private clouds."*

The establishment of a federation is contingent upon factors beyond its mere value, specifically involving the trust relationships among the participating cloud providers within the federation. As a result, a cloud provider's inclination to join a federation leans towards those with elevated value, constituted by cloud provider members boasting heightened trust scores. The level of trust attributed to cloud providers within a federation pertains to the degree of confidence each provider enjoys. This confidence is shaped by assessments from all fellow cloud providers within that federation, alongside feedback from users. In light of this, we define an institutional quality-aware trusted cloud federation game as a form of cooperative coalitional game, which we outline through the following steps.

4.3.2.2. Proposed Algorithm for Coalition Formation

To achieve the solution of the game, we propose in this section a distributed cooperative coalition formation algorithm that enables the requester to make a decision about which cloud service provider can be trusted and be able to collaborate to establish a federation. By filtering out potential partners based on their trustworthiness and price, the purpose of the algorithm is to create a coalition between cloud service providers. Afterward, Shapley values will be calculated for each cloud service provider based on their trustworthiness and price. There is a

concept in a cooperative game theory known as Shapley's value that assigns a value to each player based on their marginal contribution to the coalition as a whole. A requester's cloud service provider initiates the algorithm by providing the number of resources required and the price the requester is willing to pay for the resources in order to initiate the algorithm. This results in the establishment of a coalition of trusted partners among the cloud service providers as a result of this process. The proposed algorithm used both static and dynamic cloud federation formation where the static cloud federation formation is performed in the coordination service provider and the dynamic cloud federation is performed in every requester cloud service providers.

Algorithm 1: CoalitionFormation

Input: requester CSP CSP_i, required Resources $requiredResources$, Willingness to pay price WTP_{price}

Output: $CSPCoalition$ a coalition established between CSPs

$CSPList \leftarrow getFromCoor(CSP_j, info)$

$PotentialPartners \leftarrow DiscoverCSPTrust(CSP_i, CSP_j)$

$availableResource \leftarrow PotentialPartners.availableResource$

$price \leftarrow PotentialPartners.price$

for $csp \in PotentialPartners$ **do**
    if $csp.price <= WTP_{price}$ **then**
        $filteredCSPlist.append(csp)$

if $isempty(filteredCSPlist)$ **then**
    return $none$

$shapleyvalues$ =

for $csp \in filteredCSPlist$ **do**
    $shapleyvalues[csp] = 0$
    for $i \in range(len(filteredCSPlist))$ **do**
        for $coalition \in itertools.combinations(filteredCSPlist, i)$ **do**
            if $csp \notin coalition$ **then**
                $coalition = coalition + (csp,)$
                $coalitionCost = sum(c.availableResource\ c \in$coalition$)$
                if $coalitionCost <= requiredResources$ **then**
                    $shapleyvalues[csp] += (WTP_{price} - (sum(c.pricec \in coalition)/len(coalition)))/(len(filteredCSPlist) * (len(filteredCSPlist) - 1))$

$maxProfit = 0$

$maxProfitCoalition = None$

for $i \in range(1, len(filteredCSPlist) + 1)$ **do**
    for $coalition \in itertools.combinations(filteredCSPlist, i)$ **do**
        $coalition_{cost}$ = $sum(csp.availableResource)$ csp $\in cspCombination$
        if $coalition_{cost} <= requiredResources$ **then**
            $coalition_{profit} = WTP_{price} - (sum(c.pricec \in coalition)/len(coalition)))/(len(filteredCSPlist) * (len(filteredCSPlist) - 1))$
            if $min(coalition_{profit})$ ¿= *0* **then**
                $maxProfitCoalition$ = $coalition$

return $maxProfitCoalition$

In the first step of the algorithm, the coordination service provider is requested to retrieve information about available cloud service providers other that the requester (CSP_j) (steps 5 and 10). A list of potential partners is then compiled based on the trust level between CSP_i and CSP_j. The objective of algorithm 2 is to perform a trust discovery process for cloud service providers, and to prepare a list of potential cloud service providers with a trust level above the threshold that is required (steps 11 and 12). Potential partners provide their available resources and its prices (step 13 & 14). It then filters out potential partners whose prices are above the requester cloud service provider willingness to pay WTP_{price}. If the filtered list is empty, the algorithm returns "none".

If there are potential partners in the filtered list, the algorithm calculates the Shapley values for each cloud service provider in the filtered list. It first initializes a dictionary named "Shapley values" with each cloud service provider in the filtered list having a value of 0. It then iterates over each cloud service provider in the filtered list and calculates their Shapley value by iterating over all possible coalitions that the cloud service provider can join, calculating the coalition cost, and checking if the coalition cost is less than or equal to the required resources. If the coalition cost is less than or equal to the required resources, the Shapley value of the cloud service provider is updated using a formula based on

the coalition's price and size. Finally, the algorithm finds the coalition with the highest profit by iterating over all possible coalitions of the filtered list and calculating their profit. The coalition's profit is the sum of the Shapley values of all the cloud service providers in the coalition. The algorithm then returns the coalition with the maximum profit to assign the customer task (step 15). Overall, the algorithm takes in a requester cloud service provider, required resources, and willingness to pay a price and outputs a coalition established between cloud service providers with the highest profit. It filters out potential partners based on their price and calculates the Shapley values for each cloud service provider to determine their contribution to the coalition's profit. It then finds the coalition with the highest profit and returns it.

4.3.2.3. Proposed Algorithm for Potential Partners Selection

Algorithm 2 depicts the identification of potential partners for a requester cloud service provider (CSP_i) based on their trust level. The algorithm takes as input the requester cloud service provider and a set of foreign cloud service providers' (CSP_j) information from a Coor and outputs a set of potential partners whose trust value is greater than or equal to a threshold value.

Algorithm 2: Discover CSP Trust

Input: requester CSP CSP_i, a set of foreign CSP's information from Coor CSP_j

Output: $PotentialPartners$ Set of CSPs with $Trust(CSP_j) >= threshold$

```
set threshold
PotentialPartners = []
for j ∈ CSP_j do
    if Interactionhistory_j = 0 then
        N ← Requirednumberof Recommendations
        r ← positiveRecommendationof CSP_j From Coor
        s ← negativeRecommendationof CSP_j From Coor
        Initialize β1, β2, β3, β4, β5, β6
        VoA ← CSP_j From Coor
        PS ← CSP_j From Coor
        GE ← CSP_j From Coor
        RQ ← CSP_j From Coor
        RL ← CSP_j From Coor
        CC ← CSP_j From Coor
        Trust(j) ← ComputeTrustBasedonEquation.....1
        else
            getUserFeedback(j, Interactionhistory_j)
            getCSPsFeedback(j, Interactionhistory_j)
            Trust(j) ← ComputeTrustBasedonEquation.....5
    if Trust(j) >= threshold then
        add.PotentialPartners
return PotentialPartners
```

The algorithm first initializes the threshold and an empty list to store potential partners. For each foreign cloud service providers, it checks if interaction history is available. If there is no interaction history, it requests a required number of recommendations from the coordinator

cloud service provider about the foreign cloud service provider. Then six variable values are extracted from information provided by Coor and weights for the variables are introduced based on user preference. These values are used to compute institutional reputation w.r.t data protection policy, cyber security preference, and others. A trust is computed then according to Equation 1. However, if there is previous interaction history, the algorithm retrieves user feedback and cloud service provider feedback from the history and computes the trust value using Equation 5. After computing the trust value of each foreign cloud service provider, the algorithm checks if the value is greater than or equal to the threshold value. If it is, the foreign cloud service provider is added to the potential partner's list. Finally, the algorithm returns the set of potential partners.

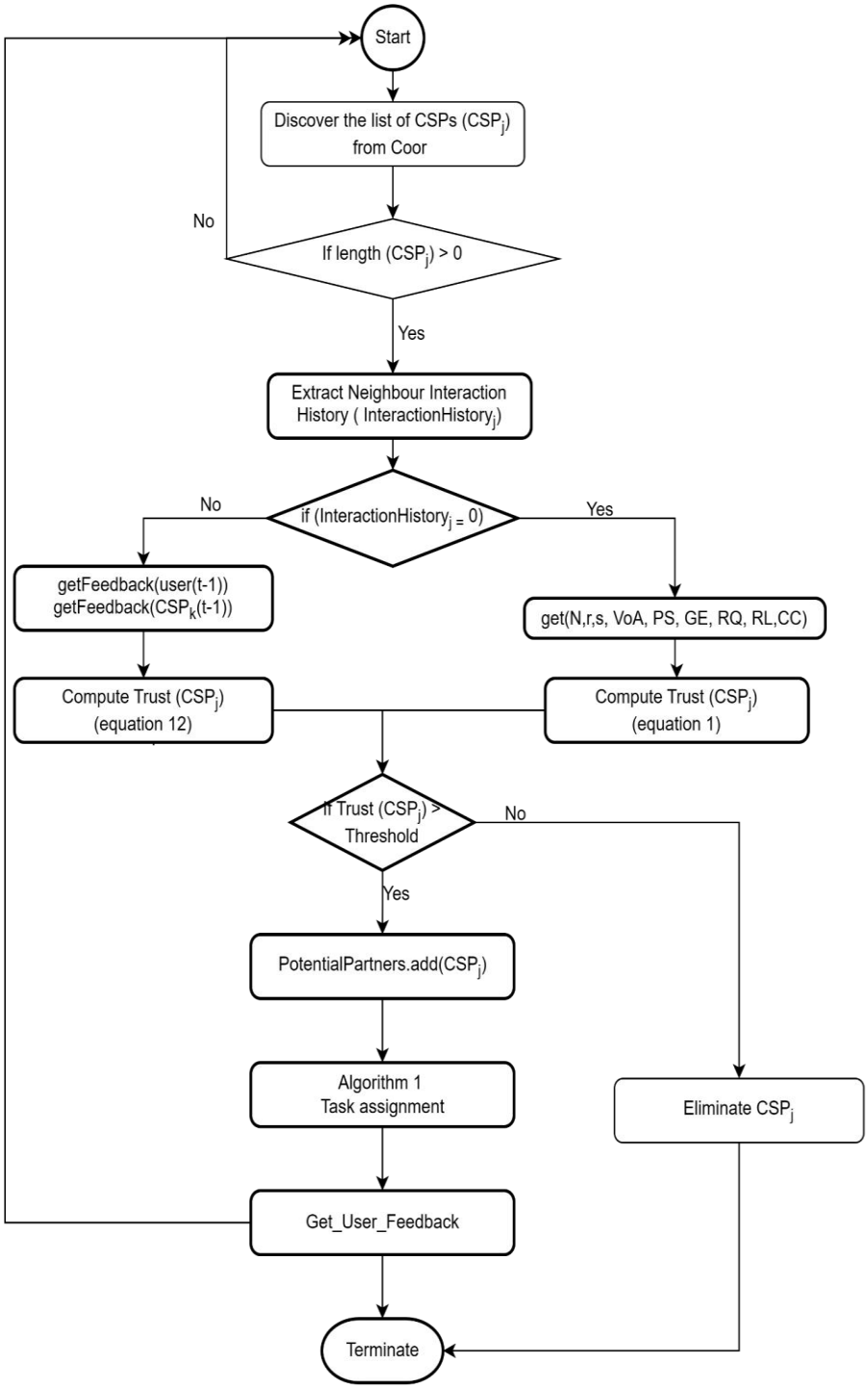


Figure 4.4: The proposed trust evaluation model flowchart

4.3.3. Trust Evaluation Models

This part shows the details of how the trust evaluation indicated in Figure 4.3 Step 12 is performed by each cloud service providers. The proposed trust evaluation model is formulated into two parts. Figure 4.4 presents the process and flowchart of the trust computation in algorithm 2. The first part is the initial trust evaluation when limited or no information is available. The second part is the trust evaluation based on evidence. Trust establishment is a series and repetitive process of trust computation between cloud service providers (see Figure 4.4). The process describes the step-by-step procedure of how the participant cloud providers perform in selecting another trustworthy partner from a set of cloud providers when there is limited or no information, and where there is evidence to compute.

Table 4.3: Notation

Symbol	Description	Value Range	Parameters Source
$\boldsymbol{CSP_j}$	One of the providers in the federation whose trustworthiness is being evaluated	[1 … n]	Several related works
CSP_{Rep}^{j}	The reputation of one of the providers in a federation	[0 … 1]	Computed from r_j and s_j

r_j	Represents the number of good recommendations given	$r_j \epsilon \Re \geq 0$	(Mashayekhy et al., 2021) (Wahab et al., 2018) (Dhole et al., 2016)
s_j	Represents the number of bad recommendations given	$s_j \epsilon \Re \geq 0$	(Mashayekhy et al., 2021) (Wahab et al., 2018) (Dhole et al., 2016)
N	The number of expected recommendation givers	$r_j + s_j \leq N$	(Mashayekhy et al., 2021) (Wahab et al., 2018) (Dhole et al., 2016)
IQ_{Rep}^{j}	The index of institutional quality based on world bank data and normalized to the value between 0 and 1	[0 … 1]	Computer from VoA_j, PS_j, GE_j, RQ_j, RL_j and CC_j
VoA_j	Voice of Accountability	[0 … 1]	Worlds Governance Indicator
PS_j	Political Stability no violence	[0 … 1]	Worlds Governance Indicator
GE_j	Government Effectiveness	[0 … 1]	Worlds Governance Indicator
RQ_j	Regulatory Quality	[0 … 1]	Worlds Governance Indicator
RL_j	Rule of Law	[0 … 1]	Worlds Governance Indicator
CC_j	Control of Corruption	[0 … 1]	Worlds Governance Indicator
$Trust_{t=0}^{i \to j}$	Initial trust computed from recommendation and institutional quality	[0 … 1]	Computer from CSP_{Rep}^{j} and IQ_{Rep}^{j}

$Trust_{t=k}^{i\to j}$	Trust computed at $t = k$ time	[0 … 1]	Computed from $IndirectTrust_{t=1}^{i\to j}$
$CS(F_{t=k}^{CSP_i\to j})$	It is the confidence score of feedback from peer cloud service provider at $t = k$	[0 … 1]	(Mujawar & Bhajantri, 2022)
$CS\ (F_{t=k}^{user_j\to j})$	It is the confidence score of feedback from user at $t = k$	[0 … 1]	(Meng & Zhang, 2020)
β	The weight given for the $Feedback_{t=0}^{CSP_i\to j}$ as well as IQ_{Rep}^{i} parameters	[0 … 1]	Assumption
α	The weight given to direct trust	[0 … 1]	Assumption
$F_{t=0}^{i\to j}$	Direct trust of CSP_i towards CSP_j based on direct interaction feedback at time $t = k$	[0 … 1]	Gartner's review and computed from $F_{t=0}^{CSP_i\to j}$
$F_{t=k}^{user_j\to j}$	The Feedback based trust computed based on the feedback collected after the user interaction at time $t = k$	[0 … 1]	Computed from $Feedbacks_{user_i\to j}(QoS$

$F_{t=k}^{CSP_i \rightarrow j}$	The Feedback from peer cloud service provider based trust computed based on the feedback collected after the peer cloud service provider interaction at time $t = k$	[0 … 1]	Computed from $Feedbacks_{CSP_i \rightarrow j}(Bhv)$
$Feedbacks_{user_j \rightarrow j}(QoS)$	The average of all feedback from the CSP_j 's user to CSP_j and each user gives feedback of 1 to 5 for each QoS parameters by rating CSP_j wrt QoS parameters	[1 … 5]	Gartner's review, (Mujawar & Bhajantri, 2022)
$Feedbacks_{CSP_i \rightarrow j}(Bhv)$	The average of all feedback of peer CSP_i given to CSP_j and each CSP_i gives feedback of 1 to 5 for each behavioural parameters by rating CSP_j	[1 … 5]	(R. Latif et al., 2021) (Mujawar & Bhajantri, 2022)
$IndirectTrust_{t=1}^{i \rightarrow j}$	Indirect trust of CSP_j computed from feedbacks from user and peer providers	[0 … 1]	Computer from
$num\_QoS_{Par}{}^{j}$	The number of user whom their job J is assigned to the CSP_j resources	[1 … n]	Assumption

$num\_Bhv_{par}{}^{j}$	the number of cloud service provider's in the coalition partner with the CSP_j	[1 … n]	Assumption
$max(feedback_{value})$	This variable represents the maximum feedback that will be given by cloud service provider. As the maximum feedback is 5, the value will be the number of feedback givers multiplied by 5.	5	Gartner's review portal
$min(feedback_{value})$	This variable represents minimum feedback that will be given by cloud service provider. The minimum feedback value is 1 and the value will be the number of feedback givers multiplied by 1.	1	Gartner's review portal

We consider a system model in which a set on n number of CSPs $\cup_1^n (CSP) = \{CSP_1, CSP_2, \ldots, CSP_n\}$ where each CSP $CSP_i \epsilon \cup_1^n (CSP)$ contributed a maximum number of available resource instances $R = \{R_1, R_2, \ldots, R_n\}$ to the cloud federation. User submitted a required resource request to execute their application on the cloud resource. In this context, the cloud federation involves multiple cloud providers collaborating to fulfill the demands of each application. Every application requires VM instances of the same type, and a specific

job is assigned to each VM instance, as is commonly practiced. The cloud providers work together and coordinate their efforts to execute these jobs (J) by undertaking all necessary measures to ensure the protection of user data during the execution process. One of these measures is being a trusted cloud provider. For individual cloud providers, establishing trust is crucial to building a strong reputation, increasing customer loyalty, and expanding their business. Since a single provider has a resource limitation, it might ask for cooperation with others to rent the ideal resources from partners by establishing a cloud federation. As trust is an important factor for the success of such cooperation, selecting a trusted partner is also one of the important tasks that need to be done carefully. In the case of cloud federation, trust evaluation can be challenging, especially during the partner selection stage without the previous interaction history. Cloud providers may have to rely on limited information and third-party evaluations or references to evaluate the trustworthiness of potential partners. Moreover, building trust among cloud providers in a federation requires careful consideration of various factors. Therefore, this study develop a model to evaluate the trust of cloud providers in two stages during the partner selection process: when there is limited information and when there is enough information.

4.3.3.1. Step One: Initial Trust Evaluation based on limited information

The most important phase of cloud providers in the cloud federation to develop trust is at the beginning of their interaction (MCKNIGHT et al., 1998). Therefore initial trust is crucial for the success of this collaboration. For the first stage of cloud service providers' trust evaluation, we propose trust as a subjective probability, especially during the partner selection stage with incomplete information that is subjected to uncertainty. Hence to present the trust model, we used the CertainTrust model proposed by (Ries, 2007, 2009)as the foundation to computer the proposed trust evaluation model. The CertainTrust model (refer to (Ries, 2009) for details) employs opinions (subjective information) to model the trustworthiness of agents, which express one's belief in the truth of a specific proposition or a combination of propositions. For instance, an agent's trustworthiness can be evaluated based on its ability to provide a particular service with an agreed-upon level of quality, or quality and timeliness.

The CertainTrust model computes the trustworthiness of an entity using opinions that are represented by a triple of values, denoted as o = (t, c, f). The value t represents the average rating, which in this study is represented by the cloud service provider reputation (CSP_{Rep}^{j}) (see section 4.3.3.1.1), and is computed based on the positive or negative

recommendation collected from peer cloud service providers. This recommendation is gathered with the help of Coop, the trusted coordinator, and forwards the number of positive and negative recommendations to the requester cloud service provider. The value f represents the initial expectation assigned to the statement's truth and in this study, it is represented by institutional quality reputation (IQ_{Rep}^{j}) and is computed using six different factors (see section 4.3.3.1.3). In the original model, the initial expectation is given randomly, but this also has another issue in case of less number of recommendations which leads to relying on the initial trust. However, instead of giving a random initial trust, this study brought another perspective to utilize their institutional reputation to extend the cloud service provider at least to behave as its external environment or institution. The value c, indicates the degree of certainty associated with the average rating given from peer cloud service providers.

Each opinion o = (t, c, f) or ($CSP_{Rep}^{j}, c, IQ_{Rep}^{j}$) is also associated with expectation value, i.e. a point estimate, taking in to account initial expectation ($f = IQ_{Rep}^{j}$) , the average rating ($t = CSP_{Rep}^{j}$), and the certainty c as follow:

$$E(t, c, f) = t * c + (1 - c) * f$$

From now on it represented as:

$$Trust_{t=0}^{i\to j}(CSP_{Rep}^{j}, c, IQ_{Rep}^{j}) = CSP_{Rep}^{j} * c + (1 - c) * IQ_{Rep}^{j} \quad \textbf{(Equation 1)}$$

Where:

- $\boldsymbol{Trust_{t=0}^{i\to j}(CSP_{Rep}^{j}, c, IQ_{Rep}^{j})} \in [0; 1]$: The cloud service provider Trust where 0 indicates the low trust level and 1 indicated the higher trust level.
- $\boldsymbol{CSP_{Rep}^{j}} \in [0; 1]$: Cloud service provider reputation based on recommendation or feedback.
- $\boldsymbol{c} \in [0; 1]$: certainty of CSP_{Rep}^{j}
- $\boldsymbol{IQ_{Rep}^{j}} \in [0; 1]$: express the institutional quality reputation where the is located. This parameter express the base trust assigned to the cloud service provider which means that the providers are expected to be at least as trusted as its institutional quality. A higher institutional quality reputation means the cloud service provider is expected to be more trustworthy

In the following section, each entity in the trust model ($Trust_{t=0}^{i\to j}(CSP_{Rep}^{j}, c, IQ_{Rep}^{j})$) is explained in detail:

4.3.3.1.1. Cloud Service Providers Reputation (CSP_{Rep}^{j})

The CertainTrust model has a component called CSP_{Rep}, which is responsible for representing the reputation of a cloud service provider. The reputation of a specific cloud service provider is determined by recommendations given to that cloud service provider. In order to select

a trustworthy cloud service provider among the available options, it is important to consider the candidate cloud service provider's past experience if there is any and/or peer opinion to predict the cloud service provider's future certainty. Although there may be various uncertainties regarding identity, collaboration context, and motivation, evaluating past direct and indirect interaction experiences is a good approach to predicting future certainty. Trust between cloud providers is measured based on their previous interaction and experience, whereas a cloud provider rates another cloud provider based on direct trust for local ratings. To evaluate the CSP_{Rep}^{j}, the recommendation is given by a value -1, 0, and 1, where -1 represents bad recommendation, 0 represents indifferent, and 1 represents a good recommendation.

The Bayesian approach for deriving trust from evidence has been previously discussed in various literature (Hosseinnezhad et al., 2021; Li et al., 2019; Shi et al., 2022; Zimba et al., 2019) though it isn't related to trust evaluation for cloud federation formation. This paper provides a brief summary of the notation and concepts that are necessary to understand the model presented. The key parameters used to calculate the trustworthiness of an entity based on evidence are the numbers of positive (r) and negative (s) evidence collected from direct evidence and recommendations. Within a specific context of an application, the opinion regarding the trustworthiness of an entity based on past experience is

represented as $\boldsymbol{CSP_{Rep}^{j}} = (\boldsymbol{r}, \boldsymbol{s})^{rs}$. It should be noted that the superscript only refers to notation. Moreover, the parameters r_0 and s_0 are introduced to indicate prior knowledge. For the parameters α and β, the beta probability density function for a random variable p is defined as h(p | α, β):

$$h(p/\alpha, \beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha)\,\Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1}$$

$$\text{Where } 0 \leq p \leq 1, \alpha > 0, \beta > 0$$

The relationship between the parameters of the beta probability density function, the collected evidence, and the prior knowledge is established by defining $\alpha = r + r_0$ and $\beta = s + s_0$. Since utility-based decision-making requires only a point estimate (Ries, 2007, 2009) and not the distribution itself, the distribution is summarized using its expected cloud service provider reputation value. The expected cloud service provider reputation value, which is the mean value of the beta distribution Beta (α, β), is given as:

$$\boldsymbol{CSP_{Rep}^{j}}(r_j, s_j, {r_j}^o, {s_j}^o) = \boldsymbol{CSP_{Rep}^{j}}(\alpha, \beta) = \frac{\alpha}{\alpha + \beta}$$

$$= \frac{r_j + {r_j}^o}{r_j + {r_j}^o + s_j + {s_j}^o}$$

Where:

- $\boldsymbol{CSP_{Rep}^{j}} \in [0; 1]$: CSP reputation based on recommendation.

- $\boldsymbol{r_j \epsilon \Re \geq 0}$: represents the number of positive recommendations given
- $\boldsymbol{s_j \epsilon \Re \geq 0}$: represents the number of negative recommendations given
- $\boldsymbol{r_j^o \epsilon \Re \geq 0}$: represents the prior number of positive recommendations given
- $\boldsymbol{s_j^o \epsilon \Re \geq 0}$: represents the prior number of negative recommendations given

In the current state-of-the-art approach (Ries, 2007, 2009), the prior knowledge r_0 and s_0 is value is considered 1 since the trust evaluation model is to be utilized in. While this approach results in a uniform distribution for the anticipated behavior of unfamiliar entities, it's crucial to recognize that this assumption is formulated by the creators of these models. Moreover, this assumption can hinder users from incorporating their individual preferences into the system. Similarly, as the proposed trust model is for the partner selection stage, our assumption is that there is no prior knowledge to compute r_0 and s_0 . Therefore, our model consider r_0 and s_0 as 0, and the models are updated as follows:

$$\boldsymbol{CSP^{j}_{Rep}}(r_j, s_j,) = \begin{cases} 0 & if\ r = s = 0 \\ \frac{r_j}{r_j + s_j} & else \end{cases} \qquad \textbf{(Equation 2)}$$

Where:

- $\boldsymbol{CSP_{Rep}^{j}} \in [0; 1]$: CSP reputation based on recommendation or feedback.
- $\boldsymbol{r_j \in \Re} \geq 0$: represents the number of positive recommendations given
- $\boldsymbol{s_j \in \Re} \geq 0$: represents the number of negative recommendations given

4.3.3.1.2. Certainty (c)

This study defines "certainty" as the level of trust that a future CSP can place in a given recommendation. The degree of certainty is determined by the evidence gathered to support the recommendation, including the number of reputable recommendation providers and their past experiences. A higher level of certainty reflects a greater degree of trustworthiness in the targeted cloud service provider, developed through prior experience with peer cloud service providers. The certainty value is expressed as a number between 0 and 1, where 0 indicates complete uncertainty and 1 indicates sufficient certainty to evaluate the cloud service provider's reputation. The final expected trust level is influenced by the average recommendation rate, with higher certainty values resulting in a greater impact on the final trust level.

$$c = \frac{N * (r_j + s_j)}{2 * (N - (r_j + s_j)) + N * (r_j + s_j)} \qquad \textbf{(Equation 3)}$$

Where:

- $\boldsymbol{N \epsilon \Re} \geq 0$: is the expected number of recommendation givers and $r + s \leq N$.
- $\boldsymbol{r_j \epsilon \Re} \geq 0$: represents the number of positive recommendations given to CSP_j
- $\boldsymbol{s_j \epsilon \Re} \geq 0$: represents the number of negative recommendations given to CSP_j

4.3.3.1.3. Institutional Reputation (IQ_{Rep}^{j})

In order to establish trust among members of an institution, it is necessary to think that the necessary impersonal structures have been put into place in order for them to be able to act anticipating a successful undertaking in the future (P. Shapiro, n.d.; Zucker, 1986). The rapid growth of cloud computing has created opportunities for organizations to improve their operational efficiency but also presents challenges around data privacy, security, and regulatory compliance, particularly for cross-border cloud federations. To overcome these challenges, organizations must establish a foundation of trust that enables effective collaboration between different cloud service providers. The institutional quality and governance index can play a crucial role in fostering institutional trust and establishing cross-border cloud federations between different cloud service providers (Law & Azman-Saini, 2012). The institutional quality and governance index measures the quality of institutions and governance

in a particular country or region, which can facilitate cross-border collaboration and investment (Robbins, 2012). By leveraging institutional quality and governance index as a measure of institutional trust, organizations can establish a foundation of trust that can enable effective collaboration and partnerships in the rapidly evolving cloud computing ecosystem.

Furthermore, this study proposes institutional reputation, which can be used as an alternative trust (initial expectation). By computing the institutional reputation along with cloud service provider reputation, the proposed model can provide an overall trust measure for cross-border cloud federation formation. A cloud federation allows multiple cloud service providers in different regions to collaborate and offer a variety of cloud services to customers. The quality of governance and institutions in a particular country is an essential factor in establishing a stable and sustainable cloud federation. Therefore, to compute the institutional, we utilized the world governance indexing indicators. The governance index indicator comprises six factors that are important in establishing a country's ability to offer strong laws and regulations that promote data security and privacy. These factors are reflected in the Voice of Accountability (VoA), Political Stability no violence (PS), Government Effectiveness (GE), Regulatory Quality (RQ), Rule of Law (RL), and

Control of Corruption (CC). A cumulative IQ_{Rep}^{j} is designed for the purpose of computing institutional reputation as follows:

$$IQ_{Rep}^{j} = \beta_1 VoA_j + \beta_2 PS_j + \beta_3 GE_j + \beta_4 RQ_j + \beta_5 RL_j + \beta_6 CC_j \quad \textit{(Equation 4)}$$

Where :

- The values of VoA, PS, GE, RQ, RL, and CC is within the range of [0,100] and $\beta_1+\beta_2+\beta_3+\beta_4+\beta_5+\beta_6=1$.
- ***IR*** (Institutional Reputation) is a dependent variable computed to observe the institutional quality.
- $\boldsymbol{VoA_j}$ (Voice of Accountability) represents the perceptions regarding the degree to which citizens of a country can engage in the process of selecting their government, along with the level of freedom they have in expressing themselves, forming associations, and accessing free media.
- $\boldsymbol{PS_j}$ (Political Stability no violence) denotes the measure of perceptions concerning the probability of political instability and the occurrence of politically-motivated violence, including acts of terrorism. This indicator reflects the extent to which a country is perceived to maintain political stability and remain free from violent disruptions.
- $\boldsymbol{GE_j}$ (Government Effectiveness) reflects perceptions of the quality of public services, the quality of the civil service and the degree of its independence from political pressures, the quality of

policy formulation and implementation, and the credibility of the government's commitment to such policies.

- $\boldsymbol{RQ_j}$ (Regulatory Quality) represents the perceptions of various aspects related to the government's performance. This indicator encompasses the quality of public services provided, the effectiveness and independence of the civil service from political influences, the proficiency in policy formulation and implementation, and the credibility of the government's commitment to its policies. It offers an assessment of how well the government operates and fulfills its responsibilities in these critical areas.
- $\boldsymbol{RL_j}$ (Rule of Law) represents the perceptions regarding the level of confidence and adherence to societal rules by various agents. This indicator encompasses the quality of contract enforcement, protection of property rights, the efficiency of law enforcement agencies and the judicial system, as well as the likelihood of crime and violence within the society. It provides insights into the extent to which the rule of law is upheld and respected in a given country or region.
- $\boldsymbol{CC_j}$ (Control of Corruption) represents the perceptions concerning the degree to which public authority is wielded for personal benefit, encompassing both minor and major instances of

corruption, as well as the influence of privileged groups and private interests in co-opting state institutions. This indicator offers insights into the effectiveness of measures taken to prevent and combat corruption within a society, including the prevention of undue influence by powerful elites and private entities over the state.

The measurement of institutional reputation involves assigning varying weights to six different indexes, and it is a subjective assessment influenced by the preferences of the cloud service providers. Different cloud service providers may assign different levels of reputation to a particular institution due to the assigned weights and their own preferences regarding the parameters. In every scenario, a cloud service provider would select one institution over another to determine which institution can be considered institutionally trusted or not based on their individual metrics. Therefore institutionally trusted and not trusted is defined as follow.

Institutionally trusted (from a cloud service provider perspective): An institution that is considered trustworthy, reliable, and reputable by a specific cloud service provider based on their individual interests, preferences, and evaluation criteria. This institution aligns with the cloud service provider's requirements, values, and objectives, and is perceived as a reliable partner for establishing federation.

Institutionally not trusted (from the cloud service provider perspective): An institution that is not regarded as trustworthy, reliable, or reputable by a specific cloud service provider based on their individual interests, preferences, and evaluation criteria. This institution does not align with the cloud service provider's requirements, values, or objectives, and is seen as unreliable or lacking the necessary attributes to be considered institutionally a reliable partner for establishing federation.

4.3.3.2. Step Two: Updating Trust Evaluation based on QoS parameter as evidence

Trust development is a continuous stage even after the interaction is established. Once enough information is available that helps to evaluate the trust based on evidence, trust computation will continue utilizing this evidence. Therefore updating the candidate cloud service provider's trust level is necessary to expand the network after the first interaction at the time t = 0 has occurred. The trust value at time t = 1 is determined by calculating the feedback-based trust using the provided feedback from the previous interaction, along with the trust established at time t = 0.

At the second stage, this study introduces a two-sided feedback evaluation approach to assess both QoS parameters from users after completing a job and peer-review feedback from partner cloud service providers concerning the providers' behavioral trust. The QoS

parameters encompass factors like response time, availability, and reliability of the provided cloud services. Collecting feedback related to QoS parameters enables Coor to assess the service quality of each cloud provider and identify any potential issues.

Moreover, the study suggests obtaining feedback from partner cloud service providers regarding the behavioral trust of the cloud providers. This peer-review feedback considers factors such as the cloud provider's willingness to collaborate, transparency, and commitment to the partnership. By gathering peer-review feedback, the study aims to evaluate the behavioral trust of each cloud provider and incorporate it into the overall feedback assessment. $at\ time\ t = 0, the\ trust\ is\ evaluated\ as\ shown\ in\ equation\ 1$

After calculating the initial trust $Trust_{t=0}^{i\to j}(CSP_{Rep}^{j}, c, IQ_{Rep}^{j})$ and forming the coalition, the user task will be assigned to CSP^j . Subsequently, feedback about the CSP^j is gathers from the user and all peer providers. This feedback is then used to compute the trust based on feedback $at\ time\ t = 1$ as shown in equation 5.

$$Trust_{t=1}^{i\to j} = \beta * F_{t=0}^{i\to j} + (1-\beta) * IndirectTrust_{t=0}^{i\to j} \qquad \textbf{(Equation 5)}$$

Where:

- $\boldsymbol{Trust_{t=1}^{i\to j}}$ represents the trust of CSP_i towards CSP_j at a time $t = 1$

- $\boldsymbol{\beta}$ represents the weight given for the direct interaction based trust
- $\boldsymbol{F_{t=0}^{i\rightarrow j}}$ represents the normalized direct feedback of CSP_i towards CSP_j at time t=0 based on the prior interaction. In this case $\boldsymbol{F_{t=0}^{i\rightarrow j}}$ can be taken as $\boldsymbol{F_{t=0}^{CSP_i\rightarrow j}}$ and can be computed as shown in equation 7, 9 and 11.
- $\boldsymbol{IndirectTrust_{t=0}^{i\rightarrow j}}$ represents the indirect trust computed by feedbacks gathered from users and peer providers at a time $t = 0$.

4.3.3.2.1. Feedback-based Trust Computation

To compute the $F_{t=0}^{i\rightarrow j}$ and $IndirectTrust_{t=0}^{i\rightarrow j}$, the feedbacks are collected from user interacted with the CSP_j and all peer providers at time $t = 0$ and computes as follows:

User feedback at time $t = 0$

$$Feedback_{t=0}^{user_j\rightarrow j} = \frac{\sum_{QoS=1}^{num\_QoS} (Feedbacks_{user_j\rightarrow j}(QoS)}{num\_QoS} \quad \textbf{(Equation 6)}$$

Peer providers feedback at time $t = 0$

$$Feedback_{t=0}^{CSP_i\rightarrow j} = \frac{\sum_{Bhv=1}^{num\_Bhv_{par}} Feedbacks_{CSP_i\rightarrow j}(Bhv)}{num\_Bhv_{par}} \quad \textbf{(Equation 7)}$$

Where:

- $\boldsymbol{CSP_i} \in$ ***All CSP in Coor*** $except\ j$

- $\boldsymbol{Feedback_{t=0}^{user_j \to j}}$ is the average of all feedback from the j's user to CSP_j and each user gives feedback of 1 to 5 for each QoS parameters by rating CSP_j wrt QoS parameters and compute its average by diving it to the number of parameters (num_QoS) to be considered as feedback of i's user
- $\boldsymbol{Feedback_{t=0}^{CSP_i \to j}}$ is the average of all feedback of peer CSP_i given to CSP_j and each CSP_i gives feedback of 1 to 5 for each behavioral parameters by rating CSP_j wrt behavioral parameters and take its average by diving it to the number of parameters (num_Bhv_{par}) to get $Feedback_{t=0}^{CSP_i \to j}$.
- $\boldsymbol{num\_QoS}$ is the quality of service metrics such as availability, reliability, security, that used to rate the CSP_j
- $\boldsymbol{num\_Bhv_{par}}$ are the behavioral metrics used by the peer cloud service provider to rate CSP_j

The value of $Feedback_{t=0}^{user_i \to j}$ and $Feedback_{t=0}^{CSP_i \to j}$ fall within the range of 1 to 5, where 5 indicates the CSP_j received the highest feedback from all user and peer cloud service provider and 1 indicate the CSP_j received the lowest feedback from all user and peer cloud service providers. To store the feedback in the Coor, these values are normalized using equations 8 and 9.

$$F_{t=0}^{user_j \to j} = \frac{Feedback_{t=0}^{user_j \to j} - min(feedback_{value})}{max(feedback_{value}) - min(feedback_{value})} \quad \textbf{(Equation 8)}$$

$$F_{t=0}^{CSP_i \to j} = \frac{Feedback_{t=0}^{CSP_i \to j} - min(feedback_{value})}{max(feedback_{value}) - min(feedback_{value})} \quad \textbf{(Equation 9)}$$

Where:

- $\boldsymbol{min(feedback_{value})}$ is the minimum feedback value that can be given. In this case, 1 is the minimum value which the feedback givers can give.
- $\boldsymbol{max(feedback_{value})}$ is the maximum feedback value that can be given. In this case, 5 is the maximum value which the feedback givers can give.

Therefore ∴

$$F_{t=0}^{user_j \to j} = \frac{Feedback_{t=0}^{user_j \to j} - 1}{5 - 1} = \frac{Feedback_{t=0}^{user_j \to j} - 1}{4} \quad \textbf{(Equation 10)}$$

$$F_{t=0}^{CSP_i \to j} = \frac{Feedback_{t=0}^{CSP_i \to j} - 1}{5 - 1} = \frac{Feedback_{t=0}^{CSP_i \to j} - 1}{4} \quad \textbf{(Equation 11)}$$

Next, when a cloud service provider CSP_i wants to computes its trust towards another cloud service provider (CSP_j) based on their direct interaction and indirect interaction, first the indirect interaction is computed as follow:

$$IndirectTrust_{t=0}^{i \to j} =$$

$$\alpha * \left(\frac{\sum_{user_j=1}^{numUser_j} \left[\left(F_{t=0}^{user_j \to j} * CS\left(F_{t=0}^{user_j \to j}\right) \right) + \left(Trust_{t=0}^{i \to j} * \left(1 - CS\left(F_{t=0}^{user_j \to j}\right)\right) \right) \right]}{numUser_j} \right)$$

$$+(1-\alpha)*\left(\frac{\sum_{CSP_k=1}^{numCSP-1}\left[\left(F_{t=0}^{CSP_k\rightarrow j}*CS(F_{t=0}^{CSP_k\rightarrow j})\right)+\left(Trust_{t=0}^{i\rightarrow j}*\left(1-CS(F_{t=0}^{CSP_k\rightarrow j})x\right)\right)\right]}{numCSP-1}\right)$$

(Equation 12)

Where

- $\boldsymbol{F_{t=0}^{user_j\rightarrow j}}$ is the feedback gathered from the CSP_j's user ($user_j$) and normalized as shown in equation 10.
- $\boldsymbol{CS}\ (\boldsymbol{F_{t=0}^{user_j\rightarrow j}})$ represents the confidence score of the collected feedback from the CSP_j's user ($user_j$) and computer as shown in equation 14.
- $\boldsymbol{numUser_j}$ represents the number of users under CSP_j.
- $\boldsymbol{user_j}$ represents the CSP_j's user.
- $\boldsymbol{F_{t=0}^{CSP_k\rightarrow j}}$ represents the feedbacks that CSP_k provides about CSP_j considering that CSP_i is the requester cloud service provider. This feedback is collected specifically to calculate the indirect trust of CSP_i towards CSP_j based on the assessments received from other peer providers CSP_k and computed as shown in equation 11.
- $\boldsymbol{CS}(\boldsymbol{F_{t=0}^{CSP_k\rightarrow j}})$ represents the confidence score of the feedback given from CSP_k to CSP_j and computed as shown in equation 16.
- $\boldsymbol{Trust_{t=0}^{i\rightarrow j}}$ represents the initial trust of CSP_i towards CSP_j and computed as shown in equation 1.

- $\boldsymbol{numCSP}$ represents the number of cloud service provider registered under Coor except the requester cloud service provider.

The confidence score of user's feedback $CS\ (F_{t=0}^{user_j \to j})$ and peer providers feedback $CS(\ F_{t=0}^{CSP_k \to j})$ is computed as shown in section 4.3.3.2.2. Furthermore, the above computation shows how the trust is evaluated at time $t = 1$. To represent the trust computation at $t = a$, we follow the same process.

At time $t = 2$ $Trust_{t=2}^{i \to j} = \beta * F_{t=1}^{i \to j} + (1 - \beta) * IndirectTrust_{t=1}^{i \to j}$

time $t = 3$ $Trust_{t=3}^{i \to j} = \beta * F_{t=2}^{i \to j} + (1 - \beta) * IndirectTrust_{t=2}^{i \to j}$

$\vdots$

time $t = a$

$$Trust_{t=a}^{i \to j} = \beta * F_{t=a-1}^{i \to j} + (1 - \beta) * IndirectTrust_{t=a-1}^{i \to j} \quad \textbf{(Equation 13)}$$

Where

- $\boldsymbol{IndirectTrust_{t=a-1}^{i \to j}} = \alpha *$

$$\left(\frac{\sum_{user_j=1}^{numUser_j} \left[\left(F_{t=a-1}^{user_j \to j} * CS\ (F_{t=a-1}^{user_j \to j}) \right) + \left(Trust_{t=a-1}^{i \to j} * \left(1 - CS\ (F_{t=a-1}^{user_j \to j}) \right) \right) \right]}{numUser_j} \right)$$

$$+(1 - \alpha)$$

$$* \left(\frac{\sum_{CSP_k=1}^{numCSP-1} \left[\left(F_{t=a-1}^{CSP_k \to j} * CS(\ F_{t=a-1}^{CSP_k \to j}) \right) + \left(Trust_{t=a-1}^{i \to j} * \left(1 - CS(\ F_{t=a-1}^{CSP_k \to j}) x \right) \right) \right]}{numCSP - 1} \right)$$

- $\boldsymbol{F_{t=a-1}^{user \to j}}$ is computed according to equation 10
- $\boldsymbol{F_{t=a-1}^{CSP_i \to j}}$ is computed according to equation 11

- $\boldsymbol{IndirectTrust}_{\boldsymbol{t=a-1}}^{\boldsymbol{k\rightarrow j}}$ is computed according to equation 12
- $\boldsymbol{a} \boldsymbol{\epsilon} \boldsymbol{\Re}^{+}$, $\beta, \alpha \ \epsilon\ [0,1]$ and $k > 0$
- $\boldsymbol{numUser_j}$ is the number of users whom their job J is assigned to the CSP_j at $t = a$.
- $\boldsymbol{numCSP}$ is the number of cloud service provider's registered in the Coor except CSP_i at time $t = a$

Therefore for each time $t = a$ the trust of $CSP_k \ towards \ CSP_j$ is computed as shown in equation 13.

4.3.3.2.2. Confidence Score Computation

Confidence scores in feedback from users and peer providers are essential for building a reliable trust evaluation model. It helps in assessing feedback authenticity, allowing for weighted aggregation, increasing robustness to manipulation, providing contextual interpretation, and enabling model calibration. Higher confidence scores indicate more reliable feedback, while lower confidence scores may suggest uncertainty or speculation. Confidence scores can also be used as weights in aggregating feedback, making the model more robust to manipulation, and providing additional context for interpreting feedback. It can also be used for model calibration, improving the trust evaluation system's accuracy and reliability over time. Incorporating confidence scores is crucial for developing a reliable trust evaluation model that fosters trust in online interactions and transactions. Therefore, this study

incorporates the confidence score of feedback to ensure that the trust evaluation is accurate and reliable.

To measure the confidence score for users' and peer providers' feedback, the heuristic approach is used for the user feedback confidence score based on feedback deviation from the prior trust and threshold. On the other hand, a weight-based confidence score approach is used for feedback from peer providers. The confidence score computation for user feedback compares the deviation of the normalized feedback from the prior trust and the threshold value. This is due to the fact that trust is a gradual process. It gradually changes over time as more interactions and feedback are provided (Edelenbos & Klijn, 2007; Grillitsch & Nilsson, 2022; Kramer, 1999; Weber et al., 2004). Furthermore, the deviation approach can give a comprehensive and balanced view of customer satisfaction and loyalty. Therefore, the user feedback certainty can be determined by the variation from the prior trust and threshold. The user feedback provided consistently with high deviations from prior trust values or thresholds considers biased or inconsistent in their assessments, which can negatively affect trust development. Additionally, when feedback is highly variable, it can be difficult to determine which feedback is reliable and which is not. By using a measure such as the deviation of feedback from the prior trust level and

the expected threshold, it may be possible to identify feedback that is consistent with the prior trust level and the expected threshold.

On the other hand, the certainty of feedback from a peer provider can be measured by the weight of the feedback giver (Mujawar & Bhajantri, 2022). This approach computes the weight for each cloud service provider based on the requester cloud service provider prior trust towards these cloud service providers and the weight is calculated and compared with the total cloud service provider trust. Once the weight is determined, it is considered as an individual feedback giver weight and the user as a confidence score for computing the trust for the next interaction. Therefore, the confidence score of user feedback and peer providers' feedback is computed as shown in equations 14, 15 and 16. The confidence score for user's feedback ($CS\,(F_{t=0}^{user_j \to j})$) and peer providers' feedback $CS(\,F_{t=0}^{CSP_i \to j})$ is presented as follow:

$$CS\,(F_{t=0}^{user_j \to j}) = 1 - \left[\frac{\left(\left|Trust_{t=0}^{j} - F_{t=0}^{user_j \to j}\right| + \left|threshold - F_{t=0}^{user_j \to j}\right|\right)}{2}\right] \qquad \textbf{(Equation 14)}$$

$$w_{csp_{i \to k}} = \frac{Trust_{t=0}^{i \to k}}{\sum_{i=1}^{numCSP} Trust_{t=0}^{i \to k}} * F_{t=0}^{CSP_k \to j} \qquad \textbf{(Equation 15)}$$

$$CS(\,F_{t=0}^{CSP_k \to j}) = \frac{1}{1 - log(w_{csp_{i \to k}})} \qquad \textbf{(Equation 16)}$$

For the t=a, the confidence score is calculated as follow:

$$CS\,(F_{t=a}^{user_j \to j}) = 1 - \left[\frac{\left(\left|Trust_{t=a}^{i \to j} - F_{t=a}^{user_j \to j}\right| + \left|threshold - F_{t=a}^{user_j \to j}\right|\right)}{2}\right] \qquad \textbf{(Equation 17)}$$

$$w_{csp_{i\to k}} = \frac{Trust_{t=a}^{i\to k}}{\sum_{i=1}^{numCSP} Trust_{t=a}^{i\to k}} * F_{t=a}^{CSP_k\to j} \quad \text{for} \quad n>1$$

$$CS(F_{t=a}^{CSP_k\to j}) = \frac{1}{1-log(w_{csp_{i\to k}})} = \frac{1}{1-log\left(\frac{Trust_{t=a}^{i\to k}}{\sum_{i=1}^{numCSP} Trust_{t=a}^{i\to k}} * F_{t=a}^{CSP_k\to j}\right)} \quad \textbf{(Equation 18)}$$

4.4. Experiment

In this section, we explain the experimental setup used to perform our simulation and the study of the performance of the IQ-aware trusted cloud federation formation based on a cooperative coalition game by means of simulation experiments. Two experiments are conducted using NetLogo for the first experiment and Python for the second experiment. The first experiment is aimed to examine the impact of institutional quality on cloud service providers' trust and cloud federation formation and the second experiment is aimed to examine the trust source credibility for trust aggregation and its effect on cloud federation formation. We use a comparative experiment using scenario-based approach to compare the performance and effect of the proposed model towards the cloud federation formation compared with other models.

4.4.1. Initial Trust Evaluation (Experiment 1)

We have conducted our experiment on Intel(R) Core(TM) i7-10510U CPU @ 1.80GHz 2.30 GHz processor with 16 GB of RAM in a 64-bit Windows 11 environment. To experiment with the institutional quality of the cloud federation formation, we used the NetLogo

simulation tool by representing the individual cloud providers as a node and the link between them as an established cloud federation. The first part of our experiment focused on examining the relationship between institutional quality and overall trust levels, as expressed in equation 1. Specifically, This experiment aimed to answer the first research question by determining how the variable IQ_{Rep}^{j} impacts $Trust_{t=0}^{i \to j}$. This analysis was crucial in assessing whether accounting IQ_{Rep}^{j} could benefit small-scale cloud service providers.

4.4.1.1. Scenario Description

The objective of experiment 1 is in order to examine the effect of IQ on overall cloud service provider Trust in cloud federation formation. This analysis is important, especially for small-scale providers located in countries with different levels of IQ. As of January 2023, the top 3 cloud providers with their regional and zone availability are AWS in 26 regions and 84 zones, followed by Azure in 60 regions and 116 zones, and Google Cloud in 34 regions and 103 zones. This shows that the cloud markets are controlled by the giant cloud providers and the existing trust evaluation for cloud federation has leveraged the large providers. Especially in the partner selection stage, the existing trust evaluation favors the large providers. This is because large providers have more visibility and brand recognition in the market which can create a perception of trustworthiness. However, small-scale providers may not

have the same level of visibility or reputation which creates uncertainty and distrust.

Therefore, the proposed trust evaluation model incorporates additional trust sources that the small-scale providers leverage from and get the opportunity to participate in a cloud federation. We hypothesized that small-scale providers face significant challenges in establishing a strong reputation, particularly when competing with large-scale providers. As a result, we consider small-scale providers to have low reputations or high reputations with low certainty. Given their relative obscurity, they may be less likely to receive positive recommendations, which can further impact their reputation (CSP_{Rep}^{j}).

Therefore to assess the effect of IQ presence in the trust evaluation model especially when limited information is available, we designed three scenarios. Three scenarios are designed to represent the simplified context of the real-world scenario as a hypothetical cloud market and are presented as follows.

- *In **scenario one**, a coalition is being formed by cloud providers with a high number of positive recommendations and a high IQ index.*

  According to world governance data (The World Bank, n.d.), a country with a high institutional quality index is likely to have strong governance systems, stable political environments, and

reliable legal frameworks that facilitate business growth. A reputation for providing high-quality services, building customer loyalty, and attracting new customers can be established by cloud service providers operating in such countries. Additionally, cloud service providers that have earned positive recommendations from their customers are likely to have a competitive advantage in the market, as businesses prefer providers that consistently meet their needs and expectations. Accordingly, the first scenario focuses on how the trust model evaluates and creates a coalition with such a cloud service provider.

- *In **scenario two**, a coalition is being formed by cloud providers with a high number of positive recommendations and a low IQ index.*

  A low IQ index may suggest weak governance systems in this context. This could affect cloud service providers' ability to deliver quality services. In spite of that, cloud service providers may have gained a high level of trust from their customers, which could facilitate the formation of coalitions. There are a number of African cloud providers, such as SS&C BluePrism (Inc, n.d.), AC Cloud(*Quem Somos – Angola Cables*, n.d.), and AZ Cloud(*About – AZ Cloud*, n.d.), which are local African providers located in Angola with low governance indexes as of 2021(The

World Bank, n.d.), and are having good customer reviews as well as partnering with several cloud providers. Taking this into account, this scenario represents such cloud providers that have a good reputation and have good customer reviews, but are located in the least developed countries with low levels of governance and poor standards of services. The reliability of cloud service providers is also influenced by the degree of trustworthiness that can be attributed to their individual members, which is also a critical factor when judging the reliability of the cloud service providers. While a cloud service provider with a high reputation may have earned high levels of trust, it is critical to assess the certainty of this trust to ensure that it is well-founded and can be sustained over time. Additionally, it is possible for a cloud service provider with a good reputation located in a low IQ country to be a part of a coalition, regardless of their country's institutional quality. As long as the cloud service provider has earned a solid reputation based on the quality of its services, it can be a reliable partner in the coalition. This second scenario is used to examine how reputational certainty affects coalition formation in such real-world contexts.

- In ***scenario three***, a coalition is being formed by cloud providers with a high number of negative recommendations and a high IQ index.

  The third scenario can be interpreted as a representation of a real-world situation where small-scale cloud service providers located in high-IQ countries may struggle to compete with larger cloud service providers in terms of reputation and customer recommendations. In this context, the high IQ index may suggest that the country has strong governance systems, stable political environments, and reliable legal frameworks, which provide a favorable environment for cloud service providers to establish their businesses. However, smaller cloud service providers may not have the resources or market reach to compete with the larger cloud service providers in terms of customer recommendations. This may result in negative feedback from customers and peers. The formation of a coalition in this scenario may be a strategy for smaller cloud service providers to overcome resource scarcity challenges and earn a positive reputation. By working together, smaller cloud service providers can pool their resources and expertise to develop new services or solutions, improve their business processes, and address the root causes of customer dissatisfaction. However, it is important to consider the cause of

their low reputation before establishing a coalition. Therefore, this scenario aimed to analyze the effect of IQ in the presence of reputational certainty.

4.4.1.2. Scenario Representation and Configuration

The scenario described in the previous section need to be represented in NetLogo simulation to capture all the necessary contexts. Table 4.4, shows this representation and gives values for the variable.

To assess the effect of IQ on the overall trust evaluation for cloud federation formation, the coalition size, Average cloud service provider Trust and Mean of cloud federation trust regarding the federation are utilized as the evaluation metric. The evaluation is performed to compare the result of the proposed model with another model called the General Trust Model (GTM) proposed by (Filali & Yagoubi, 2015).

$$Coalitional\ Size\ = \sum_{j\ \epsilon\ CF}^{num}\ CS\mathrm{P_j}$$

$$Trust(CSP_i) = \frac{\sum_{j\epsilon\ CF_i}^{n}\ Trust_{t=0}^{i->j}}{n}$$

Coalitional trust (average cloud federation Trust) =

$$\frac{\sum_{i\ \epsilon\ CF}^{num}\ (Trust(CSP_i))}{num}$$

Table 4.4. (Experiment 1) Simulation Setup and Configuration

Variable	Scenario-1: high number of positive recommendations and a high IQ index	Scenario-2: a high number of positive recommendations and a low IQ index	Scenario-1: a high number of negative recommendations and a high IQ index
Num	100	100	100
N	100	100	100
$\boldsymbol{r}$	[50,100]	[50,100]	[1,49]
$\boldsymbol{s}$	[1,49]	[1,49]	[50,100]
$\boldsymbol{VoA_j}$	[0.5, 1]	[0, 0.5]	[0.5, 1]
PS_j	[0.5, 1]	[0, 0.5]	[0.5, 1]
GE_j	[0.5, 1]	[0, 0.5]	[0.5, 1]
RQ_j	[0.5, 1]	[0, 0.5]	[0.5, 1]
RL_j	[0.5, 1]	[0, 0.5]	[0.5, 1]
CC_j	[0.5, 1]	[0, 0.5]	[0.5, 1]

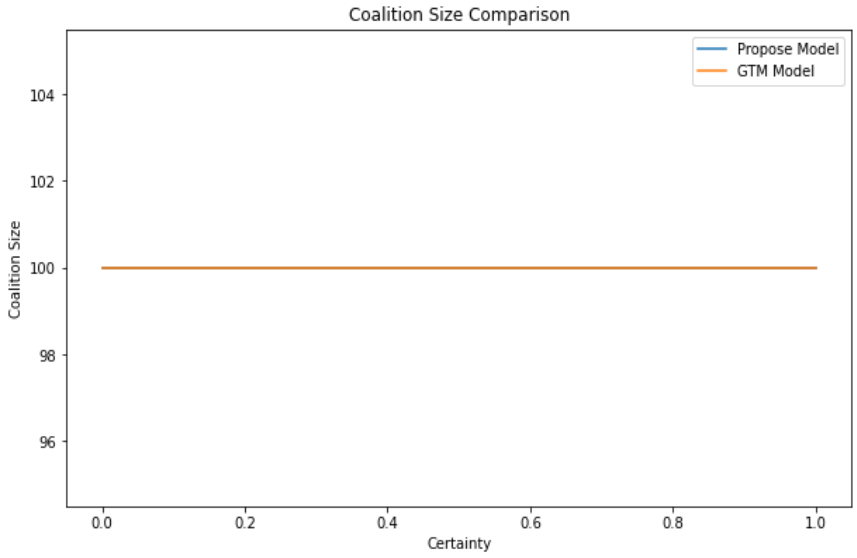
4.4.1.3. Result and Analysis

As a first step, an experiment is conducted in order to answer RQ1. For the purpose of measuring the effectiveness of the proposed trust evaluation model, we used coalition size, cloud service provider's trust and average coalitional trust. Coalition size is used to measure institutional trust's impact on cloud federation formation during uncertainty. We analyzed how institutional trust affects cloud federations formation by potentially eliminating risky cloud service providers. In

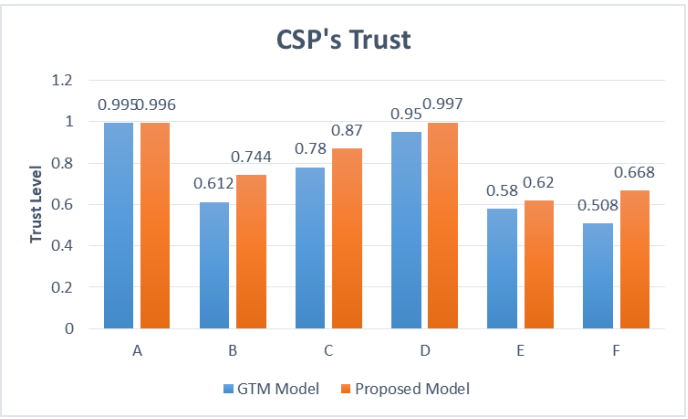
addition, the proposed model enables cloud service providers with low cloud service provider trust and uncertainty but high institutional trust to participate in cloud federation given their institutional trust as a guarantee. Furthermore, individual cloud service provider trust and average coalitional trust (cloud federation trust) were used to measure the impact of institutional trust on the overall trust evaluation process and decision-making for cloud federation formation compared with the GTM model, which does not incorporate institutional trust as one of the trust sources.

4.4.1.3.1. Coalition Size

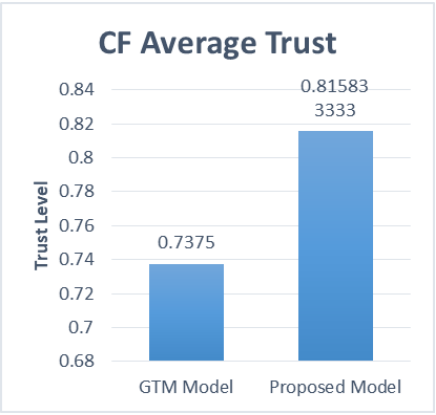
Scenario One: In this scenario, there are two models being compared for the formation of a coalition of cloud providers. The first model uses positive recommendations and a high IQ index to select the providers, while the second model uses the providers' reputation to compute trust. The comparison of these two models is done based on two factors: the number of providers in the coalition, individual cloud service provider trust and the average coalitional trust. The results show that the number of providers in both models is similar, meaning that the two models select the same number of providers for the coalition.



a)



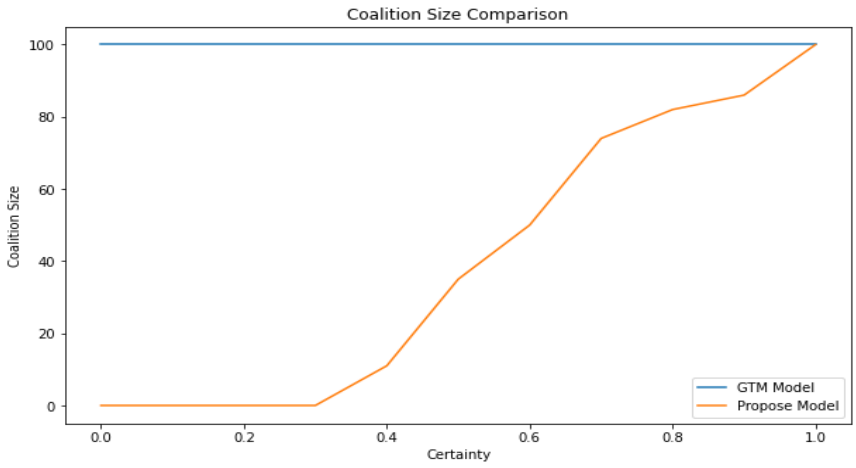
b)



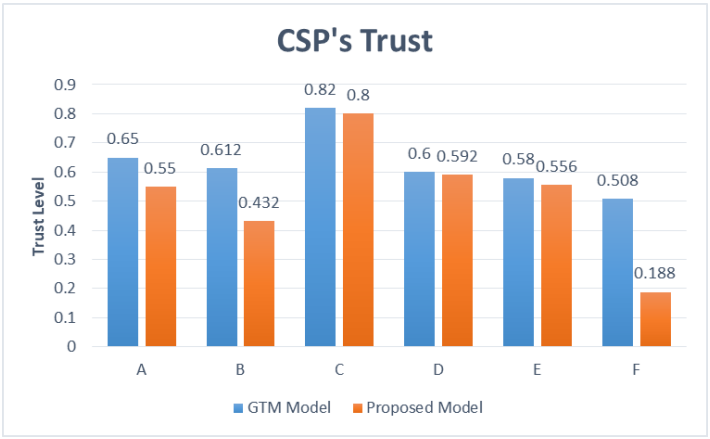
c)

Figure 4.5: a) The coalitional size of the two model b) & c) cloud service provider and cloud federation average trust respectively

Furthermore to see the effect of institutional trust in the cloud federation formation, we employ the average trust evaluation for individual cloud service provider's as well as the average trust of the cloud federation. as show Fig 4.5.b. The proposed model shows a high level of individual cloud service provider's as well as cloud federation trust. This is due to the fact that, in the presence of high institutional trust, the cloud service provider will minimize the uncertainty with the institutional quality instead of predicting the expected trust during uncertainty.



a)



b)

c)

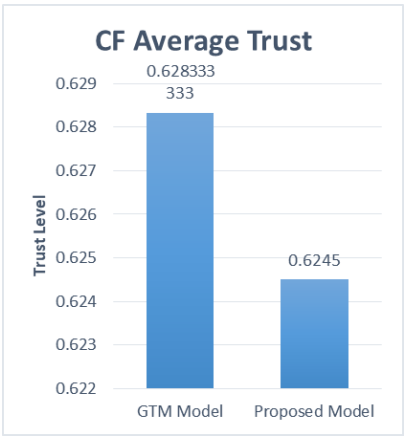
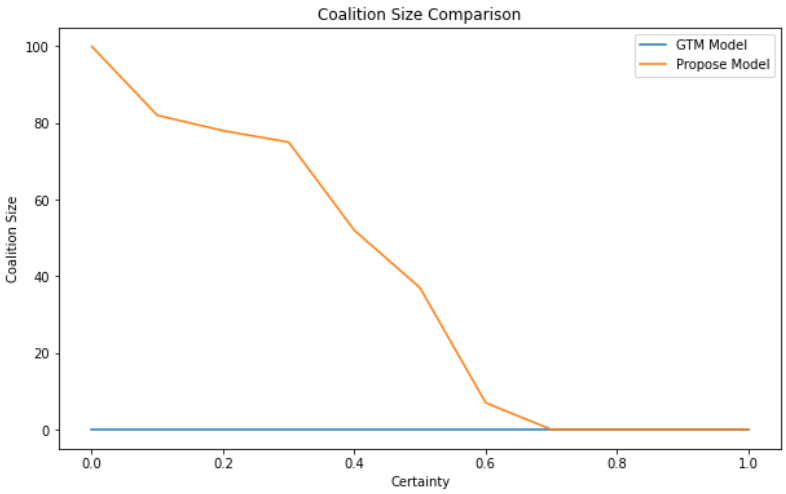


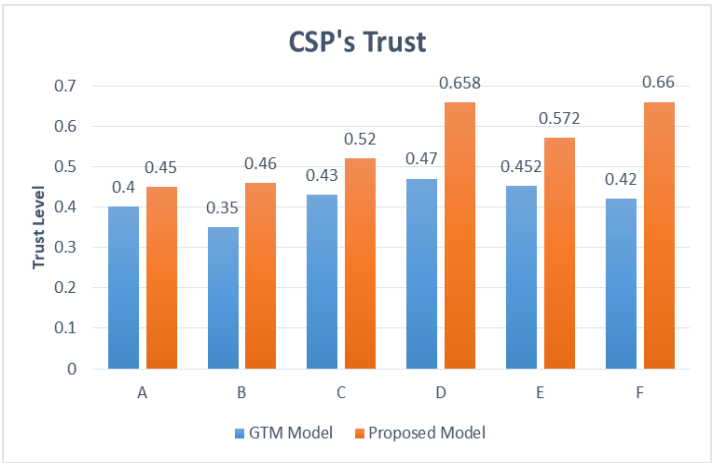
Figure 4.6: a) The coalitional size of the two models b) & c) cloud service provider and cloud federation average trust respectively

Scenario Two: The result shows that the proposed trust evaluation model, which considers the certainty level of individual reputation and institution quality, is more effective in selecting reliable and trustworthy cloud providers for the coalition compared to the other model, which establishes a coalition with all cloud service providers without considering their reputation certainty level. When the certainty level is low (0 to 0.4), the proposed model does not establish a coalition, indicating that the model is cautious about selecting providers with uncertain reputations. However, when the certainty level is higher than 0.4, the model establishes a coalition with a few cloud service providers. The higher the certainty level, the higher the number of cloud service providers in the coalition. Overall, the proposed model appears to be more effective in selecting reliable and trustworthy cloud providers for the coalition, as it takes into account the certainty of individual reputation.

Scenario Three: The results show that the proposed model can form coalitions among cloud service providers when the level of certainty is low, indicating that there is a high degree of uncertainty (Fig 4.7 a. Certainty < 0.7) about the trustworthiness of the individual cloud service providers. This is accomplished by relying on institutional trust, which is based on institutional reputation, rather than solely on individual cloud service provider trust.



a)



b)

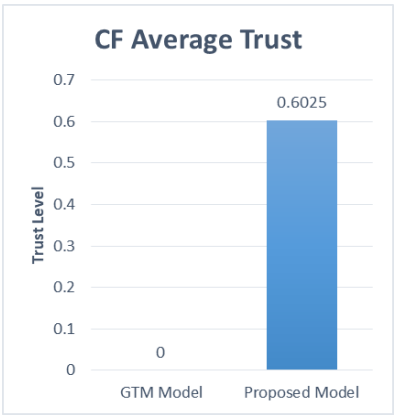
c) 

Figure 4.7: a) The coalitional size of the two models b) & c) cloud service provider and cloud federation average trust respectively

As a result, the proposed model can overcome the uncertainties associated with individual cloud service provider trust and form coalitions when overall trust in cloud service providers exceeds a certain threshold. However, if individual cloud service provider trust is both low and certain (Fig 4.7 a. Certainty > 0.7), overall cloud service provider trust falls below the threshold, and a coalition cannot be formed. Furthermore, the analysis of cloud service provider trust and coalition trust demonstrates that the proposed model is capable of establishing a significant amount of trust among cloud service providers, which is a positive outcome of the model. The GTM model, on the other hand, is unable to form coalitions due to a lack of individual trust.

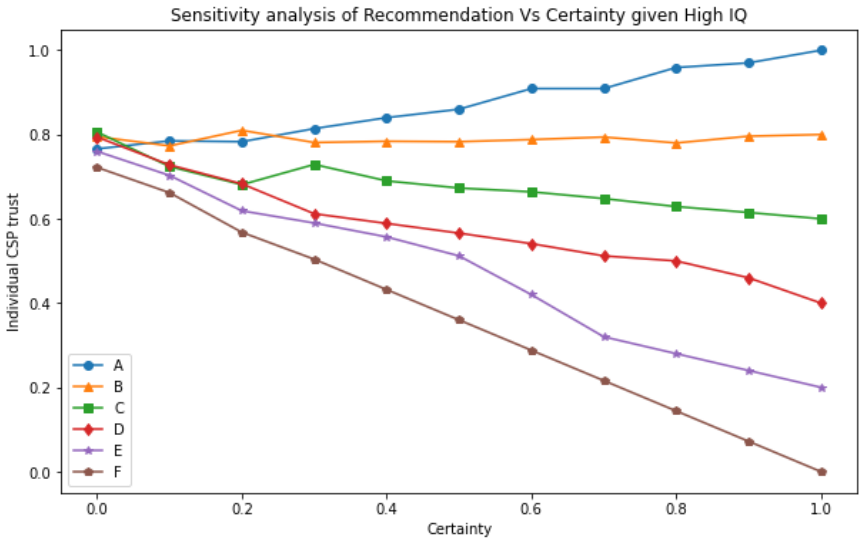
4.4.1.3.2. Sensitivity Analysis

The sensitivity analysis of individual cloud service provider trust and certainty has been performed for this model in order to evaluate the

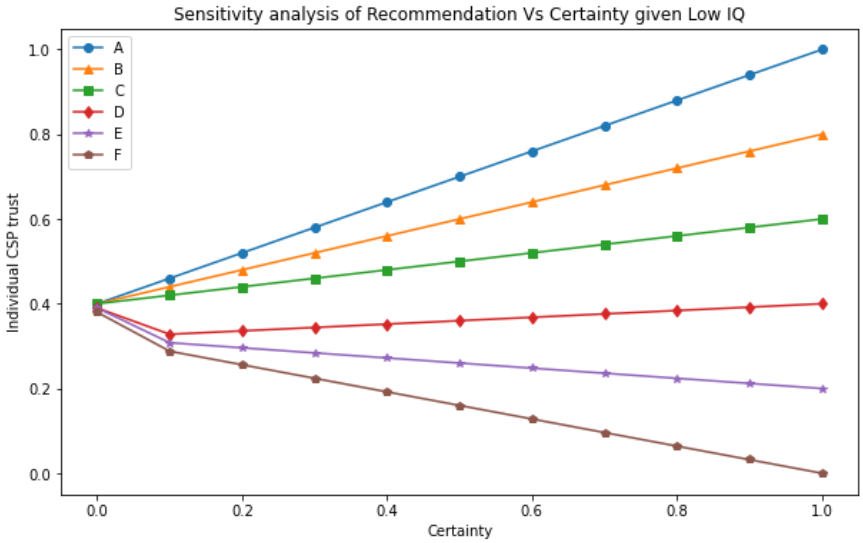
overall trust level by providing a different number of good and bad recommenders. In the following table 4.5 cases have been given for the recommendation given high and low IQ.

Table 4. 5: Recommender assumption for sensitivity analysis

Case	**Recommender's setting**
A	100% +ve recommender with 0% -ve recommender
B	80% +ve recommender with 20% -ve recommender
C	60% +ve recommender with 40% -ve recommender
D	40% +ve recommender with 60% -ve recommender
E	20% +ve recommender with 80% -ve recommender
F	0% +ve recommender with 100% -ve recommender



a)



b)

***Figure 4.8*:** a) sensitivity analysis given high IQ w.r.t certainty b) sensitivity analysis given low IQ w.r.t certainty

The results of the sensitivity analysis show (Figure 4.8) the average coalition trust level for each recommender setting and certainty level. Trust levels for each recommender setting are represented by different line colors and styles. As shown in the graph, the individual cloud service provider trust level generally increases as the percentage of positive recommenders' increases and the percentage of negative recommenders' decreases. This trend is consistent across all levels of certainty, with the trust levels being highest for setting A (100% positive recommenders) and lowest for setting F (100% negative recommenders).

However, certainty's impact on the individual cloud service provider trust levels varies depending on the recommendation setting. For example, in setting A, the trust level is already quite high even at low levels of certainty, while in setting F, the trust level remains consistently

low across all levels of certainty. This suggests that the quality of recommendations (positive vs negative) has a greater impact on trust levels as well as the level of certainty. Overall, the sensitivity analysis provides valuable insights into the factors that influence trust levels in this model and can help inform decisions about optimizing the recommender system for different contexts and user needs.

4.4.2. Trust Evaluation based on Evidence (Experiment 2)

Similar to experiment I, we have conducted our experiment on Intel(R) Core(TM) i7-10510U CPU @ 1.80GHz 2.30 GHz processor with 16 GB of RAM in a 64-bit Windows 11 environment. For this experiment, we used a Python program to implement the algorithm and compare the proposed trust evaluation with another one proposed by different authors.

The main aim of the evaluation is to establish fair cloud federations that treats all cloud providers fairly, regardless of their popularity. We also investigate how the confidence score affects partner selection in a different scenario and how it helps minimize malicious feedback and cloud service providers (Cloud Service Providers). Additionally, we aim to observe the effect of malicious feedback, particularly false feedback, on the participant cloud service provider and cloud federation formation.

4.4.2.1. Scenario Description

The proposed trust evaluation model aims to select potential partners based on their trust levels to establish a coalition. Cloud service providers can be evaluated and chosen for a coalition based on the trustworthiness of their services. The model allows for continuous evaluation of cloud service provider trustworthiness, considering both peer and user feedback.

The objective of this experiment is to evaluate the feedback-based trust evaluation model proposed in step two. The experiment aims to demonstrate the model's performance in identifying trustworthy cloud service providers and detecting malicious feedback and malicious cloud service providers based on the results.

Furthermore, the experiment aims to assess the effect of the feedback confidence score in different scenarios and observe how it influences partner selection. It also aims to evaluate the effectiveness of the proposed feedback-based trust evaluation model in identifying trustworthy and malicious service providers. By simulating various levels of maliciousness probability, the experiment will assess how the trust level varies and how long it takes to detect malicious cloud service providers and eliminate them from potential partners.

Additionally, the experiment aims to gain insight into how well the model assesses the trustworthiness of potential partners. This

evaluation can help identify any limitations or areas for improvement in the model, and inform future developments to enhance the support for secure and trustworthy cloud federations.

To do so, we have designed three scenarios.

- **Scenario one:** is to represent the requester cloud service provider had high feedback to the potential partners according to their previous interaction and it again receives high feedback from users and from peer providers.

  A scenario that examines the effect of varying confidence scores when direct trust (feedback) is high along with the feedback from cloud service provider and user. The experiment aims to assess the effect of changing the confidence score between 0 and 1 in the potential partner selection process. The confidence score for feedback from cloud service provider and the user is computed based on the weight of cloud service provider based on their trust, and the deviation from prior trust and threshold respectively. As the confidence score varies, it can impact the selection of potential partners to establish a cloud federation based on the requester cloud service provider's needs. In practice, this scenario represents how to trust evaluation models can react to the given high feedback from direct interaction with high feedback from indirect interaction through peer providers and users. The varying

confidence score can reflect the uncertainty and complexity of the trust evaluation process and how it can affect the overall trustworthiness of the cloud federation. Assessing the effect of the confidence score can help improve the accuracy and reliability of the trust evaluation model and better support the formation of secure and trustworthy cloud federations.

- **Scenario two:** is to represent the requester cloud service provider had high feedback to the potential partners according to their previous interaction but it receive low feedback from users and from peer providers.

  The second scenario represents a situation where a cloud service provider has high feedback based on direct interactions with other cloud service providers but has low feedback from users. There may exist a situation in which the confidence score in the indirect evaluation of trust may impact the overall trust computation with direct trust. This scenario highlights the importance of considering both direct and indirect trust evaluation factors when selecting potential partners for a cloud federation. While a cloud service provider may have a strong direct reputation with other providers, low feedback from users and peer providers can indicate potential risks and vulnerabilities in their services. It also emphasizes the need to continuously

evaluate cloud service provider trustworthiness and consider a range of feedback sources. This is in order to establish secure and reliable cloud federations. This also depends on how far the requester cloud service provider is willing to take the risk and vulnerabilities in their service by representing its willingness with the α value. By simulating different scenarios with varying levels of feedback from different sources, the confidence score, and α, the proposed trust evaluation can be observed, refined, and improved to better support the selection of trustworthy cloud service providers for cloud federations.

- **Scenario three:** is to represent the requester cloud service provider had low feedback to the potential partners according to their previous interaction but it received high feedback from users and from peer providers.

  In practice when a cloud service provider is looking to form a coalition with other cloud service providers, it receives high feedback from both users and peer providers regarding the trustworthiness of potential partners. However, there is low feedback from direct interaction with the potential partners, which makes it difficult to evaluate their trustworthiness based on their own services. This scenario represents a situation where the cloud service provider has to rely on indirect feedback to

evaluate the trustworthiness of potential partners. While the feedback from users and peer providers is critical, relying solely on indirect trust can be risky especially if the recommender's trustworthiness is unknown. The cloud service provider must decide how much risk they are willing to take by assessing the recommender's confidence score and adjusting the α value and seeing the potential partners. This scenario highlights the importance of having a reliable feedback system and balancing the risks associated with indirect trust when forming a cloud federation.

4.4.2.2. Scenario Representation and Configuration

The scenario described in the above section has to be represented in simulation which is written in Python programming language and captures all the necessary contexts. Table 4.6, shows this representation and gives values for the variable.

The aim of this experiment is to answer RQ2, by analyzing the coalitional size and malicious feedback rate of the proposed trust model and compared with other models.

- $Coalitional\ Size\ = \sum_{j\ \epsilon\ CF}^{num}\ CSP_{\ j}$
- $Malicious\ feedback\ rate\ =$

$$\frac{False_{feedback}}{False_{feedback} + Trust_{feedback}}$$

- $Trust(CSP_i) = \frac{\sum_{j \in CF_i}^{n} Trust_{t=0}^{i->j}}{n}$

- Coalitional trust (average cloud federation Trust)

$= \frac{\sum_{i \in CF}^{num} (Trust(CSP_i))}{num}$

Table 4. 6: (Experiment 2) Simulation Setup and Configuration

Variable	Scenario One	Scenario Two	Scenario Three
$numCSP$	5	5	5
$numUser_j$ per each cloud service provider	5	5	5
$Feedback_{t=a}^{CSP_i \to j}$	[3, 5]	[1, 2]	[3, 5]
$Feedback_{t=a}^{user_j \to j}$	[3, 5]	[1, 2]	[3, 5]
threshold	0.5	0.5	0.5
α	0.5	0.5	0.5
β	[0, 1]	[0, 1]	[0, 1]
$Trust_{t=0}^{i \to j}$	[0, 1]	[0, 1]	[0, 1]
$F_{t=a-1}^{k \to j}$	[3, 5]	[3, 5]	[1, 2]

The analysis is conducted for the above three scenarios and the result of the proposed model is compared and analyzed with another

algorithm proposed by (Gupta & Annappa, 2016a). This algorithm utilizes the direct and indirect trust relation-based partner selection in broker-based cloud federation however, this approach doesn't considers the feedback givers certainty check. It is a trust evaluation model without a confidence score (TMWO CS). Therefore in this experiment, the proposed trust evaluation result is compared with TMWO CS model.

4.4.2.3. Result and Analysis

This experiment assesses by utilizing the coalition size, and malicious feedback detection rate in order to answer the RQ2. By analyzing coalition size, it is possible to gain insight into how the accuracy of trust aggregation and the variation in the certainty of different sources can influence the coalition size. Furthermore, the malicious feedback detection rate demonstrates how effective the proposed approach is at detecting and filtering out malicious feedback from malicious peers, malicious users, and malicious CSPs. As a result of this metric, one can gain an understanding of how well the approach can be used to identify feedback and remove it.

4.4.2.3.1. Effects of different direct and indirect feedback scores in the Coalition Size

Scenario One: The first scenario represents the requester cloud service provider having high feedback based on its previous interaction with that specific cloud service provider. In addition, the requester cloud

service provider also received good feedback value from the rest of the peer cloud service provider and user. This experiment is to show the trust evaluation model is reacting to different α and CS values.

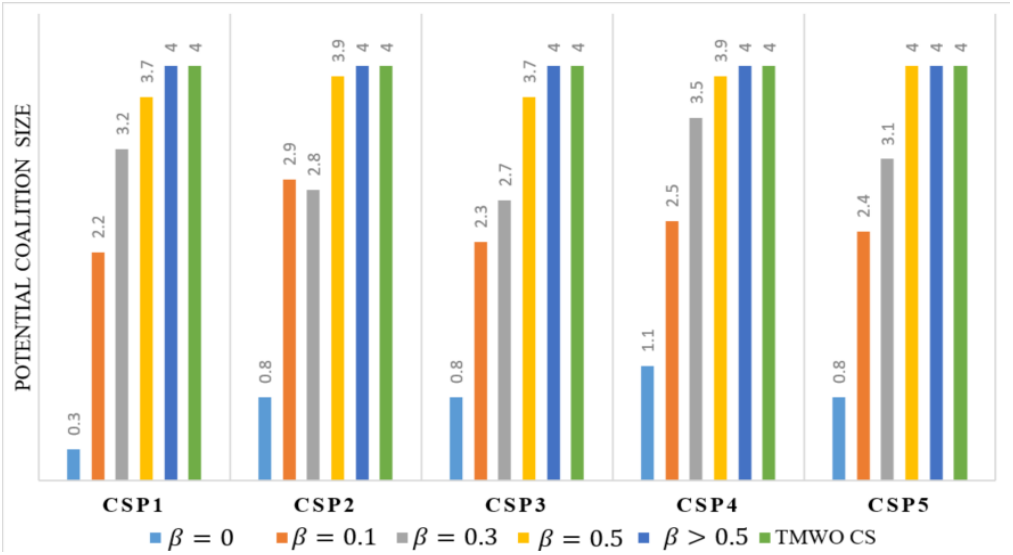


Figure 4. 9: Potential coalition size given a different β value for scenario one

The result (Figure 4.9) show that as the direct interaction and indirect interaction have high feedback value if both $CS(F_{t=a}^{CSP_k \to j})$and $CS\ (F_{t=a}^{user_j \to j})$ is high, all the cloud service provider can be potential partners regardless of the β value. However, if $CS(F_{t=a}^{CSP_k \to j})$ and $CS\ (F_{t=a}^{user_j \to j})$ is below 0.5, which is the confidence score is low as a result of low initial trust, then the partner selection relays on how much the requester cloud service provider willing to take the risk to rely indirect trust which is represented by β value. For $\beta = 0$, the requester cloud service provider is willing to take 100% risk by relying only on

one of the indirect trust. Therefore, the more the requester cloud service provider relay on direct interaction-based trust which is represented by $\beta > 0$, the number of potential partners is increased respectively. As shown in Figure 4.9, when the β value is increased so does the potential coalition size for each requester cloud service provider. Therefore the finding shows that, the coalition size is not much affected by confidence score ($CS\left(F_{t=a}^{CSP_k \rightarrow j} \right)$ and $CS\ (F_{t=a}^{user_j \rightarrow j})$) if the requester cloud service provider mostly rely on the direct trust. However, if the requester highly relies on the indirect trust ($\beta < 0$ .5)and the confidence score $CS(F_{t=a}^{CSP_k \rightarrow j})$and $CS\ (F_{t=a}^{user_j \rightarrow j})$ is lower as a result of low initial trust, the coalition size is reduces. If the previous trust above the threshold, the coalition size will be as high as the TMWOCS model. Nonetheless is the previous trust is below the threshold, the coalition size will be affected and will reduce to some extent.

Scenario Two: The second scenario represents the context when the requester cloud service provider has high feedback from the previous interaction. However, the current scenario represents the feedback from peer providers and the user is low. In this context, the cloud service provider can rely on direct trust if the requester cloud service provider has enough interaction to let it rely on direct interaction.

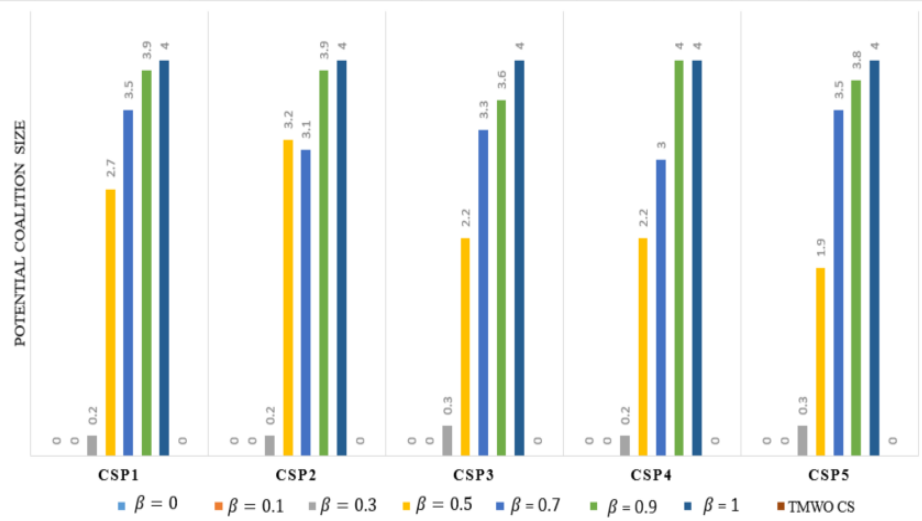


Figure 4. 10: Potential coalition size given a different β value for scenario two

However, there is also a possibility that some cloud service providers acts differently from one another even when providing similar services. This can lead to suspicion among requesting cloud service providers, who may wonder why one cloud service provider is behaving differently from another. In such cases, if the requester wants to rely on indirect trust more, the β value will be $\beta < 0.5$, and then the overall trust mainly depends on the $CS(F_{t=a}^{CSP_k \to j})$and $CS\ (F_{t=a}^{user_j \to j})$ as a result of initial trust. If the initial trust is above 0.5, the coalition size will be lower as a result of high deviation from the cloud service provider side which leads to low confidence score. Depending on the value $\beta > 0.5$, the coalition size is dependent on the initial trust as the initial trust increase so does the coalition size. As shown in figure 4.10, the key finding from the results is that the β value, which determines the

weighting of direct versus indirect interactions in trust computation, has an impact on the coalition size. When β is high, the coalition size increases, whereas a low β value, combined with initial trust, results in a smaller coalition size.

Scenario Three: The third scenario illustrates what happens when the direct interaction does not lead to a good outcome, but the rest of the providers and the users of the cloud service provider provide good feedback. As the result shown (Figure 4.11), when such situations arise the degree of certainty of the trust evaluation can be influenced greatly by β value along with the initial value. When $\beta < 0.5$ with the initial trust below the threshold, the coalition size is null. However, is the $\beta > 0.5$ regardless of the initial trust value, the coalition is created with few or more cloud service provider.

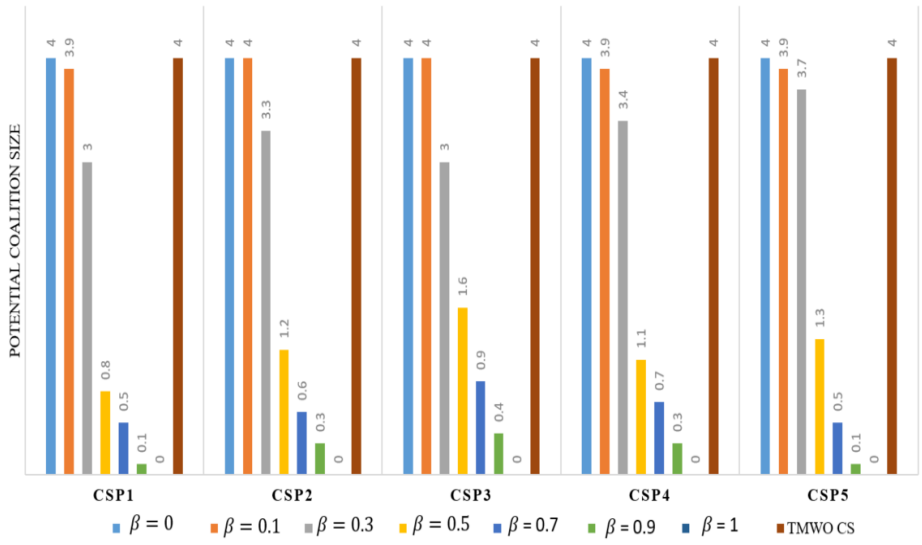


Figure 4. 11: Potential coalition size given a different β value for scenario three

It is important to realize that if the confidence score is above higher ($CS(F_{t=a}^{CSP_k \rightarrow j})$= [0.5, 1] and $CS(F_{t=a}^{user_j \rightarrow j})$ = [0.5, 1]), then the size of the potential partner is determined by how much the requester is willing to take indirect trust into account in the trust evaluation process. If the β value in Figure 4.11 is lower than 0.5, then the requester cloud service provider is likely to be able to get potential partners depending on the confidence scores values and initial trust. However, as the β value becomes even less, the more potential partners the requester will be able to get. In this case, the indirect trust will tell a potential partner how much the requester is relying on in the case of low direct trust.

4.4.2.3.2. Malicious Feedback Detection

In this experimental section, we observe if the proposed trust aggregation model identifies the malicious feedback coming from the user and peer cloud service provider given different direct and indirect feedback scores. Malicious feedback here refers to the intentional exaggeration or manipulation of scores or evaluations by a feedback giver, where the degree of maliciousness is influenced by both the extent of exaggeration from the previous score and the level of trust placed in the feedback giver. It is assumed that the same observation can be applied to all cloud service provider requests for partners. In this context, malicious feedback is defined as feedback that comes from an uncertain source or that is received with low feedback confidence. To filter out

malicious feedback from trustworthy feedback, a threshold-based detection method is used. The threshold-based detection method involves setting a threshold value for the confidence score, below which feedback is considered untrustworthy or malicious. In Figure 4.12, our proposed model identifies the malicious feedback from the given total feedback in each iteration. This is due to the fact that the proposed model measures the confidence score for each user and peer cloud service provider feedback received, and depending on the confidence score threshold, the feedback is considered to compute the trust aggregation otherwise, the prior trust is utilized as an alternative to the feedback.

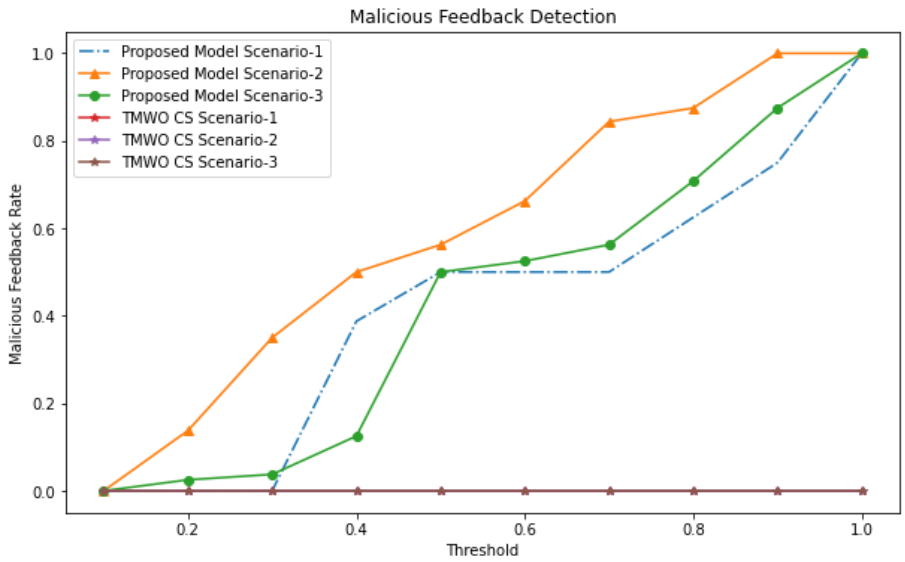


Figure 4. 12: Comparison of the proposed Model with TMWO CS model

Figure 4.12. Illustrates the malicious feedback rate detections both by the proposed model and TMWOCS. The result shows, the

proposed model effectively detected malicious feedback as compared TMWOCS. Especially, when the indirect trust is lower (second scenario), the proposed model checks if the trust is above the threshold and the feedback certainties are also above the threshold. In this scenario, the proposed model effectively eliminates a large number of feedbacks as the feedbacks are below the threshold, the certainty of the feedback is checked and eliminated.

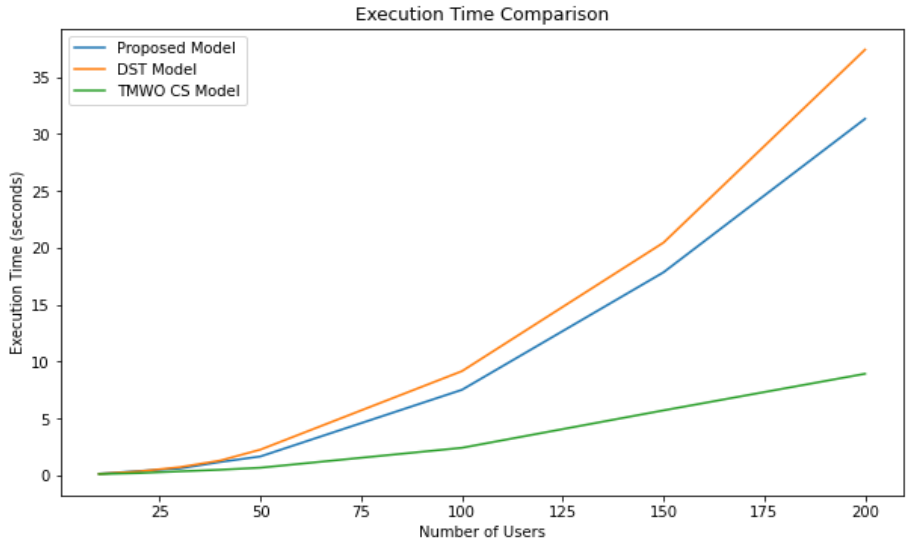


Figure 4. 13: Execution time comparison of the proposed trust aggregation model with DST and TMWO CS model

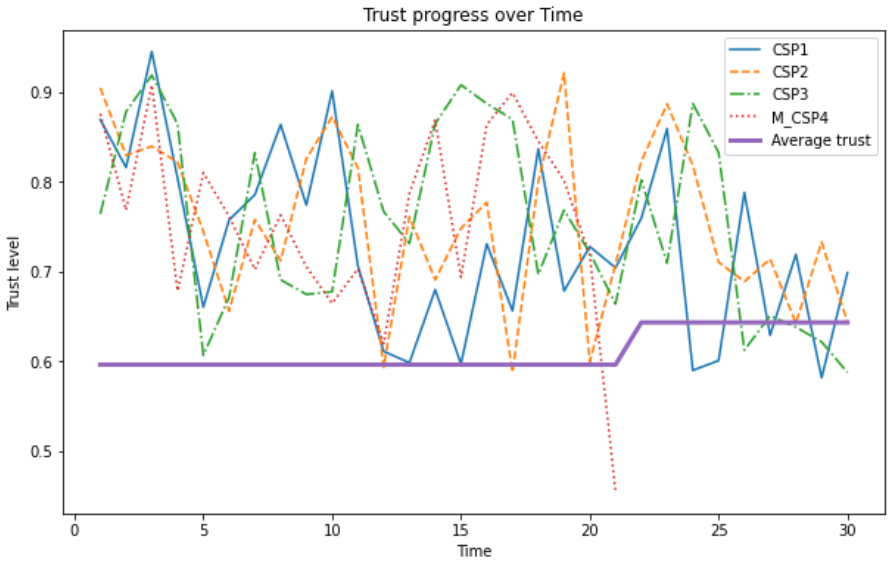
Furthermore, the execution time of is proposed model is compared with the execution time of Dempster-sheper (DST) and TMWOCS models. As shown in Figure 4.13, the proposed model shows a better performance compared with the widely used trust aggregation model DST. However, the TMWOCS model shows low execution time

and this is due to the fact that this model doesn’t apply any computation to measure the feedback credibility.

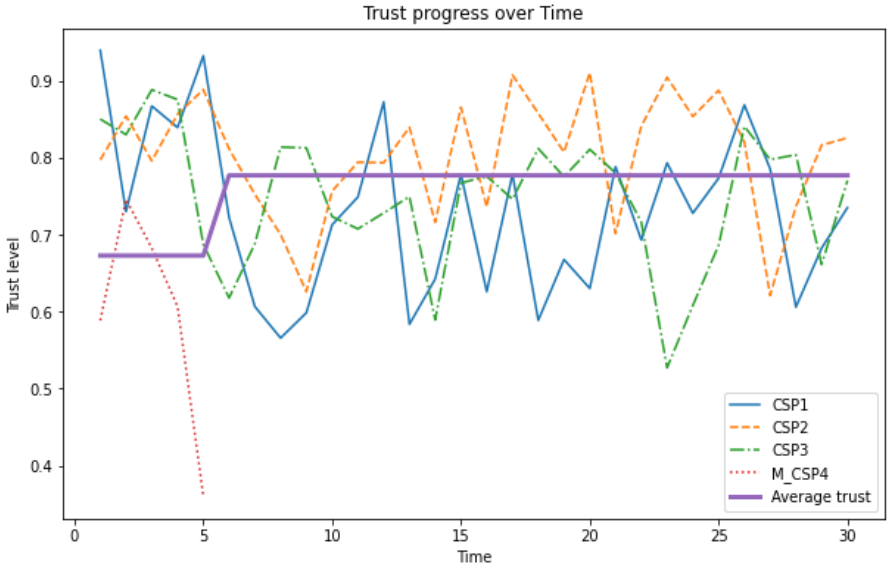
4.4.2.3.3. Average Trust of the potential partner and eliminate malicious cloud service providers.

The use of peer and user feedback for evaluating trustworthiness is a decentralized approach that reduces reliance on centralized authorities or third-party trust evaluators. This approach makes the evaluation process more transparent and accountable. Moreover, multiple sources allow a more comprehensive and accurate evaluation of cloud service providers' performance and behavior. Given the malicious feedback detection rate, we assigned different levels of maliciousness probability based on the malicious feedback provided by them and see how the cloud service provider is eliminated after a few interactions. The finding that highly malicious cloud service providers are detected after a few interactions and eliminated from the potential partner list for coalition formation before a longer iteration is consistent with the real-world scenario, where cloud service providers' malicious activities can be detected by monitoring their behavior and performance. The importance of continuous monitoring and evaluation of the cloud service providers in the coalition to identify and eliminate malicious cloud service providers before they can cause significant damage is also highlighted in the analysis. In the following experiment, the first scenario

(scenario one) setting is utilized to assess the effect of one of the cloud service provider's maliciousness probability on the potential partner's selection. The experiment is done for one requester cloud service provider looking for potential partners for 30 iteration time. The malicious cloud service provider is considered with malicious maliciousness probability and the result is observed.



a)


Trust progress over Time
Trust level
Time
CSP1
CSP2
CSP3
M_CSP4
Average trust

b)


Trust progress over Time
Trust level
Time
CSP1
CSP2
CSP3
M_CSP4
Average trust

c)

d)

Figure 4. 14: a) M_CSP4 Maliciousness probability 0.02

b) M_CSP4 Maliciousness probability 0.2

c) M_CSP4 Maliciousness probability 0.5

d) M_CSP4 Maliciousness probability 0.7

As shown in Figure 14.14, the cloud service provider with a maliciousness probability is eliminated due to the fact that the feedback from cloud service provider is given according to the cloud service provider prior interaction. This means that if the cloud service provider found to be malicious, the low feedback will be given and accordingly it will eliminate from the potential partner list.

4.5. Discussions and Implications

4.5.1. Discussions

Multi-sourced trust indicators are associated with significance and importance for trust evaluation reliability (Ahmed et al., 2019; Khan & Malluhi, 2010). Given the available evidence, it becomes crucial to provide a trust evaluation model that combines recommendations, evidence, and policy-based indicators to assess the level of trust in cloud service providers (Ahmed et al., 2019; Khan & Malluhi, 2010). As a result, the proposed model incorporates both external trust indicators and peer recommendations.

In partner selection, when trust indicators are limited, it becomes essential to have an accurate and accountable way of measuring trust, which can be accomplished by incorporating the country's reputation (institutional trust). Defining the level of risk partners are willing to take and cooperate with is critical based on the country's data privacy policy, cyber security readiness, and the rule of law. Furthermore, a study by (Clò et al., 2020) also supports that institutions significantly impacts both the quality of the external environment where firms perform their economic activity and the quality of the firm's internal governance and management mechanism. Hence, it is important to take into account the institution's reputation.

Moreover, Rossmannek et al., (2022) argue that countries with low institutional quality suffer from high levels of uncertainty in technology alliance formation. In such cases, firms rely on trust instead of institutional quality. As a result, firms use institutional quality as an alternative to uncertainty in uncertain situations. The study by (Daellenbach & Davenport, 2004; McKnight et al., 2002) supports that when the potential partners have dispositional tendencies (i.e. the interaction between potential partners is unfamiliar due to the less prior interaction(no interaction)) the institutional framework provides situational factors and the social mechanism that foster trust and trustworthiness. Therefore, institutional quality can be used to alleviate the uncertainty of the individual cloud service provider trust when less information is available and/or the cloud service provider trust computing based on this available information is uncertain.

In this regard, the experimental scenario represents a real-world scenario that analyzes the institutional quality effect in the presence of low or high trust in the cloud service provider.

To answer the first research question (***RQ1. How does incorporating institutional trust impact the overall trust evaluation process and consequently influence decision-making for cloud federation formations?****)* The first experiment is performed and analyzed the effect of the proposed model and compared with other existing

models. The analysis considers three different scenarios to test the algorithm under different conditions. In scenario one, a high number of positive feedback with high institutional quality index is evaluated. The result shows that both the trust model with and without institutional quality has established a coalition with an equal number of cloud service providers. This shows that, when the cloud service provider trust is high and certain, the effect of institutional quality is not significant. This experiment result is also supported by (F. Araujo & Ornelas, 2007; Yu et al., 2015) study that if the firms accumulate enough amount of trust, it can substitute the impact of institutional quality. In the second and third scenario, a high number of positive feedback with a low institutional quality index and a high number of negative feedback with a high institutional index is used respectively.

The result shows that depending on the certainty of the cloud service provider trust, the institutional trust impacts to asses of the overall trust. When the cloud service provider trust is high with low certainty, institutional trust is used to balance the uncertainty of the cloud service provider trust. On the other hand, if the cloud service provider trust is high and certain, the institutional trust isn't affecting the potential partner selections. It only depends on the cloud service provider trust. However, when the cloud service provider trust is high or low with less certainty, the institutional trust affects the selection of potential partners

for cloud federation formation. This is supported by (Rossmannek et al., 2022) and (Daellenbach & Davenport, 2004) studies which say the potential partners with dispositional tendencies or partners with low institutional quality can be screened by substituting the firm's trust with institutional quality and vice versa.

The proposed model responds to the second research question ***(RQ2: How do we ensure the accuracy of trust calibration in cloud federation formation when feedback collected from users and/or peer providers is subject to bias and exaggeration, including false feedback attacks?)*** By providing continuous trust evaluation systems for every transaction based on direct feedback, feedback from users and peer providers. This feedback is collected by analyzing cloud service providers' and peer providers' evaluations of the service. To ensure the credibility of the feedback, a confidence score is also introduced and calculated. This is done by comparing the normalized feedback from both sides with the previous trust and confidence threshold. The use of confidence scores as a mechanism of maintaining trust calibration is one of the most important components of many of the trust evaluation models proposed, according to (Güneş, 2021; Wei, 2017). In the context of a cloud federation formation, the confidence score (certainty measure) can be used for updating the trust level of a potential partner in a cloud federation by updating the trustworthiness of feedback from users and

peer providers. As a result of this approach, has been demonstrated to be effective at identifying malicious cloud service providers in trust evaluations and reduces the chances of false positives and false negative feedback.

The study by (Güneş, 2021; Wei, 2017)) proposed a trust evaluation model for ad-hoc networks, which introduced a confidence score that was designed to predict the certainty of the node in ad-hoc networks. In the proposed trust evaluation mode, the authors justify that accurate trust assessment plays a significant role in trust assessment and this can be achieved by incorporating certainty measure in the model. Furthermore, the study by (H. Hassan et al., 2020) introduced a covariance-based approach to determining a user's feedback credibility of cloud service provider's trust evaluation for the user to make a choice. The proposed model employs a dynamic calculation of the accumulative trust value, which is continuously updated with each transaction. This trust value represents the most recent and up-to-date evaluation of the cloud provider's performance in the cloud environment, reflecting the current state of trust based on the latest transactional interactions. In addition, the study by (Lou et al., 2018) proposes a trust assessment approaches to evaluate the manufacturing service in a cloud manufacturing environment.

This study also performs the reliability and credit assessment to measure the user feedback reliability by employing multinomial logistic regression. As discussed, several studies agreed that the confidence score is important to assess the credibility of the given feedback or subjective measure. Therefore, it justifies that, incorporating confidence score in the trust evaluation model plays a crucial role in determining the trustworthiness of cloud service providers from malicious ones and reducing false positive and false negative feedback.

Overall, the experimental analysis shows that the proposed trust model is effective in identifying potential partners for establishing coalitions based on trust even when the cloud service providers have limited information as well as based on evidence. Incorporating a confidence (certainty) score in trust evaluation models for cloud federation formation can be an effective approach to maintaining trust calibration and reducing the risk of malicious cloud service providers. This approach has been supported by studies in the literature for cloud-to-user trust. This study brings this idea by incorporating trust evaluation between cloud service providers, which hasn't been addressed by previous studies. By continuously measuring trust and updating it based on the confidence score of feedback, this approach can help to improve the accuracy and reliability of trust evaluations and enhance the security and stability of cloud federation ecosystems.

4.5.2. Implications

4.5.2.1. Practical Implications

The practical implication of the previous analysis is that institutional trust can play a crucial role in improving the certainty of subjective trust evaluations in cloud federation formation. In particular, when the cloud service provider trust is uncertain due to the limited information or biased recommendations, the institutional trust can serve as a guarantee for future cooperation and provide evidence for establishing a coalition. To improve the certainty of subjective trust evaluations, it is important to incorporate institutional trust metrics into the trust model. These metrics can include factors such as regulatory compliance, certification, and reputation of the institutions that oversee the cloud service providers. By considering these factors, the trust model can provide a more objective and comprehensive assessment of the cloud service providers, which can help to mitigate the impact of biased recommendations and other challenges that can arise in cloud federation formation.

In addition, it is important to continuously monitor and update the trust model to reflect changes in the market and evolving trust dynamics among the cloud service providers. This can be achieved through ongoing data collection and analysis, as well as feedback from the cloud service providers and other stakeholders in the cloud federation.

Therefore, by incorporating institutional trust metrics and continuously monitoring and updating the trust model, it is possible to improve the certainty of subjective trust evaluations and provide a fair assessment of all cloud service providers in cloud federation formation. Additionally, the model can be continuously updated based on feedback from users and peer providers, ensuring that the trust assessment remains accurate.

4.5.2.2. Theoretical Implications

The theoretical implication of the study is that it highlights the importance of institutional trust in assessing the level of risk partners are willing to take and cooperate with. The study suggests that when the cloud service provider trust is high and certain, the effect of institutional quality is not significant. However, when the cloud service provider trust is high or low with less certainty, the institutional trust affects the selection of potential partners for cloud federation formation. This highlights the importance of taking into account the institutional quality of potential partners in cloud federation formation.

Incorporating confidence score to maintain trust calibration has also theoretical implications. Firstly, using confidence scores can improve the accuracy of trust evaluations, reducing the risk of partnering with unreliable or untrustworthy cloud providers, and improving the overall success and effectiveness of the federation. Secondly, trust calibration can improve the accuracy of trust assessments and create

more robust and resilient cloud federations that can withstand disruptions and maintain high levels of performance and security .therefore, using confidence scores and trust calibration can enhance the theoretical understanding of trust management and create more effective and resilient cloud federations.

4.5.2.3. Managerial Implications

The study has several managerial implications for organizations involved in cloud federation formations. First, it suggests that incorporating institutional trust as a factor in the overall trust evaluation process can be beneficial in situations where there is limited information available about potential partners. This can help organizations to mitigate risks associated with uncertain situations and make more informed decisions about partner selection. Second, the study emphasizes the importance of maintaining trust calibration by continuously evaluating trust levels based on feedback from users and peer providers. This can help organizations to identify and address trust issues early on, reduce the chances of false positives and false negative feedback, and maintain the overall accuracy of the decision-making process. Third, the study highlights the need for organizations to consider a range of factors when evaluating potential partners for cloud federation formations, including data privacy policies, cyber security readiness, and the rule of law. By taking these factors into account, organizations can better assess the level

of risk they are willing to take and cooperate with and make more informed decisions about partner selection.

Finally, the study underscores the importance of developing trust evaluation models that combine recommendations, evidence, and policy-based indicators to assess the level of trust in cloud service providers. By incorporating both external trust indicators and peer recommendations, organizations can develop a more comprehensive and accurate picture of the trustworthiness of potential partners, and make more informed decisions about partner selection.

Chapter 5. Conclusion

5.1. Summary

This study aimed to answer six research questions by understanding the cloud federation formation enabling factors, requirements, challenges, and current trend emphasis on institutional quality-aware distributed trust evaluation for cloud federation formation. These research questions are answered by two main studies. To answer the first four research questions a systematic literature review approach is utilized aimed to study the key elements of cloud federation formation (chapter 3). Sixty-three primary articles are identified that are relevant to answer the four research questions. As a result, 16 enabling factors, 17 requirements, and 18 major challenges for cloud federation formation have been identified. The research findings indicate that resource provisioning and flexibility are the most discussed enabling factors, while legal issues and meeting regulations are the least explored.

From the requirement aspect, trust and reputation among cloud service providers are the most explored requirement, and cloud federation stability is the main issue discussed in the studies. In terms of research trends, several kinds of game theory have been applied in the studies, followed by set theory. Most of the solutions proposed are algorithmic and based on mathematical models, with resource information and SLA parameters being the most common factors used in

the proposed solution. The authors recommend that researchers should present more data and use real-world cloud computing environments to support their findings and that more empirical experiments and industrial studies should be conducted to satisfy computing industries' needs. Finally, the systematic literature review presents implications and potential research directions with respect to these findings.

To answer the last two research questions, the second study (chapter 4) was conducted. The study proposed institutional quality-aware trusted cloud federation formation approaches, which consist of a two-stage trust evaluation that utilizes the cooperative coalition formation algorithm. The trust evaluation model incorporates institutional trust in the first stage when only limited information is available. Then in the second stage, trust aggregation is performed by utilizing the direct trust and indirect trust computed from direct feedback, feedback from other peer providers, and feedback from users. To ensure the credibility of the feedback, a confidence score is also introduced and calculated. This approach reduces the chances of false positives and false negative feedback. The evaluation was conducted in two experiments to answer the research questions separately. The first experiment result shows that, when cloud service provider trust is high and certain, the impact of institutional quality on the selection of potential partners for cloud federation formation is not significant. However, when cloud

service provider trust is high or low with less certainty, institutional trust affects the selection of potential partners for cloud federation formation.

The second experiment evaluated the proposed feedback-based trust aggregation model and assesses its effectiveness in identifying trustworthy and malicious service providers. It uses three different scenarios to simulate varying levels of feedback from different sources and assesses the impact of changing the confidence score in the partner selection process. The experiment aims to provide insight into how well the model assesses the trustworthiness of potential partners and identify any limitations or areas for improvement in the model. The experiment results show that the proposed model is effective in identifying the trusted potential partner for establishing a coalition based on trust.

5.2. Policy Implication

The detailed implication of each study are presented in chapter 3 and chapter 4. In this section, the general implication for the government and cloud service providers is presented as follows.

Policy Implication for Government:

- One policy implication of the study is that regulatory bodies and institutions that oversee cloud service providers should prioritize improving their reputation and regulatory compliance. This can be achieved by implementing stricter regulations and enforcing them effectively, as well as establishing certification programs

for cloud service providers that meet certain standards. By improving institutional trust in this way, small cloud service providers can get a fair opportunity to participate in the cloud federation regardless of popularity and then can become more trustworthy and reliable partners in cloud federations, thereby improving the overall effectiveness and success of cloud federation formations.

- The government should establish a clear and consistent regulatory framework for cloud computing that addresses the basis for data ownership, data economy, and sharing to encourage cross-border collaborations.
- The lack of studies from a knowledge-based theory perspective suggests that there is a need for further exploration in this area to establish a knowledge creation-based cloud federation. The government can encourage and fund research in this area to promote innovation and collaboration among cloud service providers.

Policy Implication for Cloud Service Providers:

- Cloud providers involved in cloud federation formations should consider institutional trust as a factor when evaluating potential partners and incorporate it into their trust evaluation models. This

can help to mitigate risks associated with uncertain situations and make more informed decisions about partner selection.

- The Cloud service providers should consider the certainty of trust factors and their potential biases when evaluating the trustworthiness of their partners. They should develop a systematic and objective evaluation framework that takes into account different types of biases and ensures that trust is based on sound and measurable criteria.
- The cloud service providers should also collaborate and coordinate with each other and with the government to foster trust and transparency in cloud federation, and to address the potential risks and challenges of sharing data and knowledge across different domains.

5.3. Limitation and Future Research

In chapter three, we restricted our search to articles published from 2016 onwards, which could impact the comprehensiveness of our results as we may have missed relevant studies published before this time frame. However, we have attempted to mitigate this limitation by incorporating the results of relevant review studies published up to 2016, as demonstrated in Section 4.2 of our report. During the data extraction process, we encountered some papers that lacked sufficient detail or did not adhere to our established protocol. As a result, we had to make certain

assumptions when collecting data. To ensure accuracy, we cross-referenced the extracted data with related studies and recorded information presented in the article. Additionally, this study focuses on research from three specific databases - Scopus, Web of Science, and ScienceDirect - and does not include similar studies from other databases. For future work, other databases shall be incorporated to address a larger perspective of cloud federation formation enabling factors, requirements, challenges, and current trends.

In chapter four, we present a trust evaluation approach for cloud federation formation, utilizing the principles of cooperative game theory. The proposed approach focuses primarily on addressing bad-mouthing and false feedback attacks, which are the most common forms of collusion attacks in cloud computing environments. However, other types of collusion attacks have not been taken into consideration in the proposed solution. In addition, we conducted an experiment to test the effectiveness of the proposed approach, using a scenario-based approach. This method involved simulating various possible scenarios to evaluate the proposed solution's ability to detect and prevent bad-mouthing and false feedback attacks. However, the proposed approach has not yet been tested with real-world data. As a result, future work should aim to improve the proposed approach by incorporating additional models that consider other types of collusion attacks.

Additionally, the proposed algorithms and models have a great deal of potential for future applications and extensions in the context of edge and IoT computing environments, in addition to their current capabilities. As a result of considering these possibilities, the trust evaluation model can be leveraged in edge-computing scenarios for real-time trust evaluation and decision-making. The localization of trust evaluation reduces latency and dependence on centralized cloud resources. Consequently, services can be delivered more efficiently and securely in edge computing environments. One notable advantage of the trust evaluation model is its ability to address false positive or false negative attacks. The model is capable of detecting malicious feedback, which is crucial for ensuring trusted decision-making in edge computing scenarios. By identifying and mitigating the impact of such attacks, the model contributes to maintaining a reliable and secure environment for decision-making processes at the edge.

A trust evaluation framework can also be extended to IoT applications to support the evaluation of trust in these applications. Establishing trust among the various stakeholders becomes increasingly important as IoT devices become more prevalent, and their integration with cloud services becomes more prevalent. In this context, the proposed approach can be used to evaluate the trustworthiness of IoT devices, data sources, and cloud service providers. This enables the

creation of secure and reliable IoT ecosystems, where trust is pivotal in ensuring data integrity, privacy, and reliable interactions among IoT components. The algorithms and models proposed can effectively address the evolving needs and challenges posed by edge computing and IoT by embracing these future applications and extensions. The trust evaluation model provides a foundation for building trustworthy and secure systems that operate at the edge while fostering reliable collaborations and interactions among heterogeneous devices, cloud services, and stakeholders.

Bibliography

Aazam, M., & Huh, E.-N. (2014). Advance resource reservation and QoS based refunding in cloud federation. *2014 IEEE Globecom Workshops, GC Wkshps 2014*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84946690645&doi=10.1109%2fGLOCOMW.2014.7063420&partnerID=40&md5=4a8e75e9212179d5a345129ee5807ace

Abawajy, J. (2011). Establishing trust in hybrid cloud computing environments. *Proc. 10th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications, TrustCom 2011, 8th IEEE Int. Conf. on Embedded Software and Systems, ICESS 2011, 6th Int. Conf. on FCST 2011*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84856193158&doi=10.1109%2fTrustCom.2011.18&partnerID=40&md5=1a68b3a35d726252e03d2f5597fccfb3

Abdo, J. B., Demerjian, J., Chaouchi, H., Barbar, K., & Pujolle, G. (2013). Broker-based cross-cloud federation manager. *2013 8th International Conference for Internet Technology and Secured Transactions, ICITST 2013*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-

84896674864&doi=10.1109%2fICITST.2013.6750199&partnerID=40&md5=6d46bf4520764f1e2ea2954046b04bf0

Abdo, J. B., Demerjian, J., Chaouchi, H., Barbar, K., Pujolle, G., & Atechian, T. (2014). Cloud federation? We are not ready yet. *Proceedings - 16th IEEE International Conference on High Performance Computing and Communications, HPCC 2014, 11th IEEE International Conference on Embedded Software and Systems, ICESS 2014 and 6th International Symposium on Cyberspace Safety and Security, CSS 2014*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84949924454&doi=10.1109%2fHPCC.2014.139&partnerID=40&md5=52d1f6ff0dcd721c8cd8e04a522925d9

Abdo, J. B., Demerjian, J., Chaouchi, H., Yared, R., & Atechian, T. (2015). Micro-economy effect on cloud federation. *GSCIT 2015 - Global Summit on Computer and Information Technology - Proceedings*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84962256945&doi=10.1109%2fGSCIT.2015.7353324&partnerID=40&md5=cb6fc5b2d40a6410c75d04df0e4d0beb

About – AZ Cloud. (n.d.). Retrieved May 20, 2023, from https://azcloud.co.ao/about/

Abreha, H. G., Hayajneh, M., & Serhani, M. A. (2022). Federated Learning in Edge Computing: A Systematic Survey. Sensors, 22(2), Article 2. https://doi.org/10.3390/s22020450

Abusitta, A., Bellaiche, M., & Dagenais, M. (2018). On trustworthy federated clouds: A coalitional game approach. *Computer Networks, 145*, 52–63.

Abusitta, A., Bellaiche, M., & Dagenais, M. (2018b). A trust-based game theoretical model for cooperative intrusion detection in multi-cloud environments. *2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, 1–8. https://doi.org/10.1109/ICIN.2018.8401625

Addya, S. K., Turuk, A. K., Satpathy, A., Sahoo, B., & Sarkar, M. (2019). A Strategy for Live Migration of Virtual Machines in a Cloud Federation. IEEE Systems Journal, 13(3), 2877–2887. https://doi.org/10.1109/JSYST.2018.2872580

Ahmed, U., Al-Saidi, A., Petri, I., & Rana, O. F. (2021). QoS-aware trust establishment for cloud federation. *Concurrency and Computation: Practice and Experience*, e6598.

Ahmed, U., Al-Saidi, A., Petri, I., & Rana, O. F. (2022). 17. QoS-aware trust establishment for cloud federation. *Concurrency and*

Computation: Practice and Experience, e6598.

Ahmed, U., Raza, I., & Hussain, S. A. (2019). Trust evaluation in cross-cloud federation: Survey and requirement analysis. In *ACM Computing Surveys* (Vol. 52, Issue 1). https://doi.org/10.1145/3292499

Ahmed, U., Raza, I., Rana, O., & Hussain, S. A. (2021). Aggregated Capability Assessment (AgCA) for CAIQ enabled Cross-cloud Federation. IEEE Transactions on Services Computing.

Al Falasi, A., Serhani, M. A., & Dssouli, R. (2013). A model for multi-levels SLA monitoring in federated cloud environment. *Proceedings - IEEE 10th International Conference on Ubiquitous Intelligence and Computing, UIC 2013 and IEEE 10th International Conference on Autonomic and Trusted Computing, ATC 2013*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84894189018&doi=10.1109%2fUIC-ATC.2013.14&partnerID=40&md5=c4e5a6e29daf69fbad71954aa609c042

Alam, A. B., Halabi, T., Haque, A., & Zulkernine, M. (2020). Reliability-based Formation of Cloud Federations Using Game Theory. *GLOBECOM 2020-2020 IEEE Global Communications*

Conference, 1–6.

Alansari, S., Paci, F., & Sassone, V. (2017). A Distributed Access Control System for Cloud Federations. *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, 2131–2136. https://doi.org/10.1109/ICDCS.2017.241

Aliyu, S. O., Chen, F., & He, Y. (2017). QoS-Aware Resource Management in SDN-Based InterClouds: A Software Cybernetics Perspective. Proceedings - 2017 IEEE International Conference on Software Quality, Reliability and Security Companion, QRS-C 2017. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85034426643&doi=10.1109%2fQRS-C.2017.77&partnerID=40&md5=76d97dca11fcb2f478b365b145e848eb

Altmann, J., & Aryal, R. G. (2020). Refinement of Cost Models for Cloud Deployments through Economic Models Addressing Federated Clouds. Palgrave Studies in Digital Business and Enabling Technologies. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85110035609&doi=10.1007%2f978-3-030-43198-3_5&partnerID=40&md5=abf0e4cf0a069a614537afda584958c3

Altmann, J., Carlini, E., Coppola, M., Dazzi, P., Ferrer, A. J., Haile, N.,

Jung, Y.-W., Kang, D.-J., Marshall, I.-J., Tserpes, K., & Varvarigou, T. (2016). BASMATI - A Brokerage Architecture on Federated Clouds for Mobile Applications. In TEMEP Discussion Papers (No. 2016132; TEMEP Discussion Papers). Seoul National University; Technology Management, Economics, and Policy Program (TEMEP). https://ideas.repec.org/p/snv/dp2009/2016132.html

Altmann, J., & Kashef, M. M. (2014). Cost model based service placement in federated hybrid clouds. Future Generation Computer Systems, 41, 79–90. https://doi.org/10.1016/j.future.2014.08.014

Anas, A., Sharma, M., Abozariba, R., Asaduzzaman, M., Benkhelifa, E., & Patwary, M. N. (2017). Autonomous Workload Balancing in Cloud Federation Environments with Different Access Restrictions. *Proceedings - 14th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2017*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85040618182&doi=10.1109%2fMASS.2017.68&partnerID=40&md5=8a0d3a9c1b7d6887ab960bcaa79c4247

Anastasi, G. F., Carlini, E., Coppola, M., Dazzi, P., Lazouski, A., Martinelli, F., Mancini, G., & Mori, P. (2014). Usage Control in Cloud Federations. *2014 IEEE International Conference on Cloud*

Engineering, 141–146. https://doi.org/10.1109/IC2E.2014.58

Andrea Margheri, Md Sadek Ferdous; Mu Yang; Vladimiro Sassone (2017). *A Distributed Infrastructure for Democratic Cloud Federations*.. 688–691. https://doi.org/10.1109/CLOUD.2017.93

Antonio, R. (2011, October 31). *Who Coined 'Cloud Computing'?* MIT Technology Review. https://www.technologyreview.com/2011/10/31/257406/who-coined-cloud-computing/

Arutyunov, V. V. (2012). Cloud computing: Its history of development, modern state, and future considerations. *Scientific and Technical Information Processing*, *39*(3), 173–178. https://doi.org/10.3103/S0147688212030082

Aryal, R. G., & Altmann, J. (2018). Dynamic application deployment in federations of clouds and edge resources using a multiobjective optimization AI algorithm. *2018 Third International Conference on Fog and Mobile Edge Computing (FMEC)*, 147–154. https://doi.org/10.1109/FMEC.2018.8364057

Aryal, R. G. (2019). Economic Models for Incentivizing the Federations of IaaS Cloud Providers [Thesis, 서울대학교 대학원]. https://s-space.snu.ac.kr/handle/10371/162029

Aryal, R. G., & Altmann, J. (2017). Fairness in revenue sharing for stable cloud federations. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85032461148&doi=10.1007%2f978-3-319-68066-8_17&partnerID=40&md5=f06b5443068d749a09e18bf59120e36a

Assis, M. R. M., & Bittencourt, L. F. (2016). A survey on cloud federation architectures: Identifying functional and non-functional properties. *Journal of Network and Computer Applications*, *72*, 51–71. https://doi.org/10.1016/j.jnca.2016.06.014

Assis, M. R. M., Bittencourt, L. F., & Tolosana-Calasanz, R. (2014a). Cloud Federation: Characterisation and Conceptual Model. 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, 585–590. https://doi.org/10.1109/UCC.2014.90

Atlas Data Federation Overview—MongoDB Atlas. (n.d.). Retrieved June 7, 2023, from https://www.mongodb.com/docs/atlas/data-federation/overview/

Aversa, R., & Tasquier, L. (2018). Monitoring and management of a cloud application within a federation of cloud providers. *International Journal of High Performance Computing and Networking*. Scopus.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85058785817&doi=10.1504%2fIJHPCN.2018.096715&partnerID=40&md5=b472b50931068b1df17ac3248208aee7

Ayachi, M., Nacer, H., & Slimani, H. (2021a). 37. Cooperative game approach to form overlapping cloud federation based on inter-cloud architecture. *Cluster Computing*, *24*(2), 1551–1577.

Ayachi, M., Nacer, H., & Slimani, H. (2021b). Cooperative game approach to form overlapping cloud federation based on inter-cloud architecture. *Cluster Computing*, *24*(2), 1551–1577.

Bairagi, A. K., Alam, M. G. R., Talukder, A., Nguyen, T. H., Hong, C. S., & others. (2016). An overlapping coalition formation approach to maximize payoffs in cloud computing environment. *2016 International Conference on Information Networking (ICOIN)*, 324–329.

Baldi, M., Chiaraluce, F., Senigagliesi, L., Spalazzi, L., & Spegni, F. (2017). Security in heterogeneous distributed storage systems: A practically achievable information-theoretic approach. *2017 IEEE SYMPOSIUM ON COMPUTERS AND COMMUNICATIONS (ISCC)*, 1021–1028.

Barreto, L., Fraga, J., & Siqueira, F. (2021). An intrusion tolerant identity

provider with user attributes confidentiality. *Journal of Information Security and Applications*, *63*, 103045. https://doi.org/10.1016/j.jisa.2021.103045

Bavier, A., Coady, Y., Matthews, C., & TU-Kaiserslautern, P. M. (2012). GENICloud and TransCloud: Towards a Standard Interface for Cloud Federates. https://www.semanticscholar.org/paper/GENICloud-and-TransCloud-%3A-Towards-a-Standard-for-Bavier-Coady/c8cbee3ad3a795ca12d0d606d54501a2bd6324c1

Bell, C. G. (1985). Multis: A New Class of Multiprocessor Computers. *Science*, *228*(4698), 462–467. https://doi.org/10.1126/science.228.4698.462

Bennani, N., Boukadi, K., & Ghedira-Guegan, C. (2014). A trust management solution in the context of hybrid clouds. *Proceedings of the Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84908407053&doi=10.1109%2fWETICE.2014.76&partnerID=40&md5=a1855310b87fd906cc7a3d4ae7851099

Berghaus, F., Wegner, T., Lassnig, M., Ebert, M., Serfon, C., Galindo, F., Seuster, R., Garonne, V., Tafirout, R., & Sobie, R. (2019).

Integrating a dynamic data federation into the ATLAS distributed data management system. EPJ Web of Conferences, 214, 07009. https://doi.org/10.1051/epjconf/201921407009

Bernabe, J. B., Perez, G. M., & Skarmeta Gomez, A. F. (2015). Intercloud Trust and Security Decision Support System: An Ontology-based Approach. *Journal of Grid Computing*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84949320205&doi=10.1007%2fs10723-015-9346-7&partnerID=40&md5=3e3efd4a87fdf30e474dfacc3801d3ed

Bernsmed, K., Jaatun, M. G., Meland, P. H., & Undheim, A. (2012). Thunder in the Clouds: Security challenges and solutions for federated Clouds. 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings, 113–120. https://doi.org/10.1109/CloudCom.2012.6427547

Bernsmed, K., Jaatun, M. G., Meland, P. H., & Undheimy, A. (2011). Security SLAs for federated Cloud services. *Proceedings of the 2011 6th International Conference on Availability, Reliability and Security, ARES 2011*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-80455144630&doi=10.1109%2fARES.2011.34&partnerID=40&

md5=db7e70b1ad8e0b3c6fad8704ecf59121

Bielawski, S., Kempe, C., McDaniel, A., Tate, A., & Harrison, J. (2015). Salesforce.com. Robins Case Network. https://scholarship.richmond.edu/robins-case-network/16

Bielawski, S., Kempe, C., McDaniel, A., Tate, A., & Harrison, J. (2015). Salesforce.com. *Robins Case Network*. https://scholarship.richmond.edu/robins-case-network/16

Biran, Y., & Dubow, J. (2019b). Confederated cloud—Design consideration for distributed utility computing system of systems. *Systems Engineering*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054687006&doi=10.1002%2fsys.21473&partnerID=40&md5=e08f557f9b963ad84f615a658b74a743

Birney, E., Vamathevan, J., & Goodhand, P. (2017). Genomics in healthcare: GA4GH looks to 2022 (p. 203554). bioRxiv. https://doi.org/10.1101/203554

Bisong, E. (2019). What Is Cloud Computing? In E. Bisong, *Building Machine Learning and Deep Learning Models on Google Cloud Platform* (pp. 3–6). Apress. https://doi.org/10.1007/978-1-4842-4470-8_1

Bohn, R. B., Lee, C. A., & Michel, M. (2020). The NIST Cloud Federation Reference Architecture. *NIST*. https://www.nist.gov/publications/nist-cloud-federation-reference-architecture

Bohn, R. B., Chaparadza, R., Elkotob, M., & Choi, T. (2022). The Path to Cloud Federation through Standardization. 2022 13th International Conference on Information and Communication Technology Convergence (ICTC), 942–946. https://doi.org/10.1109/ICTC55196.2022.9952660

Bohn, R. B., & Lee, C. (2022). The IEEE 2302-2021 Standard on Intercloud Interoperability and Federation. NIST, 2(1). https://www.nist.gov/publications/ieee-2302-2021-standard-intercloud-interoperability-and-federation

Bohn, R. B., Lee, C. A., & Michel, M. (2020). The NIST Cloud Federation Reference Architecture. NIST. https://www.nist.gov/publications/nist-cloud-federation-reference-architecture

Bonawitz, K., Eichner, H., Grieskamp, W., Huba, D., Ingerman, A., Ivanov, V., Kiddon, C., Konecný, J., Mazzocchi, S., McMahan, H. B., Overveldt, T. V., Petrou, D., Ramage, D., & Roselander, J. (2019). Towards Federated Learning at Scale: System Design.

ArXiv. https://www.semanticscholar.org/paper/Towards-Federated-Learning-at-Scale%3A-System-Design-Bonawitz-Eichner/79cf9462a583e1889781868cbf8c31e43b36dd2f

Bouchareb, N., & Zarour, N. E. (2021). 52. An agent-based mechanism to form cloud federations and manage their requirements changes. *International Journal of Grid and Utility Computing*, *12*(3), 302–321.

BRODKIN, J. (2016, December 2). *Netflix finishes its massive migration to the Amazon cloud | Ars Technica*. https://arstechnica.com/information-technology/2016/02/netflix-finishes-its-massive-migration-to-the-amazon-cloud/

Buchanan, S., & Joyner, J. (2022). Azure Arc As an Extension of the Azure Control Plane. In S. Buchanan & J. Joyner (Eds.), *Azure Arc-Enabled Kubernetes and Servers: Extending Hyperscale Cloud Management to Your Datacenter* (pp. 1–9). Apress. https://doi.org/10.1007/978-1-4842-7768-3_1

Bucklin, L. P., & Sengupta, S. (1993). Organizing Successful Co-Marketing Alliances. *Journal of Marketing*, *57*(2), 32–46. https://doi.org/10.1177/002224299305700203

Bukaty, P. (2019). The California Consumer Privacy Act (CCPA): An

implementation guide. IT Governance Ltd.

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, *25*(6), 599–616. https://doi.org/10.1016/j.future.2008.12.001

Cao, H., & Wu, C. Q. (2018). Performance optimization of budget-constrained mapreduce workflows in multi-clouds. Proceedings - 18th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, CCGRID 2018. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85050964560&doi=10.1109%2fCCGRID.2018.00039&partnerID=40&md5=81a54ca73fe31cf48cb536d4f116ce3c

Carlini, E., Dazzi, P., Lettich, F., Perego, R., & Renso, C. (2021). Cloud and Data Federation in MobiDataLab. Proceedings of the 1st Workshop on Flexible Resource and Application Management on the Edge, 39–40. https://doi.org/10.1145/3452369.3463819

Carvalho, J. O. de, Trinta, F., Vieira, D., & Cortes, O. A. C. (2018). Evolutionary solutions for resources management in multiple clouds: State-of-the-art and future directions. Future Generation Computer Systems, 88, 284–296.

https://doi.org/10.1016/j.future.2018.05.087

Casalicchio, E., & Silvestri, L. (2012). *Optimal Resource Allocation in Federated Clouds*.

Castañeda, I. A., Blanquer, I., & Dee Alfonso, C. (2019). Easing the deployment and management of cloud federated networks across virtualised clusters. CLOSER 2019 - Proceedings of the 9th International Conference on Cloud Computing and Services Science. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85067464234&doi=10.5220%2f0007877406010608&partnerID=40&md5=28b4880396510fea949bbdc08fd552df

Cayirci, E. (2013). Configuration schemes for modeling and simulation as a service federation. SIMULATION. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84887580004&doi=10.1177%2f0037549713501574&partnerID=40&md5=7ba5f4fc6641b03f9e0d33b303b8ca45

Celesti, A., Tusa, F., Villari, M., & Puliafito, A. (2010). How to enhance cloud architectures to enable cross-federation. 2010 IEEE 3rd International Conference on Cloud Computing, 337–345.

Celesti, A., Tusa, F., Villari, M., & Puliafito, A. (2012). How the

Dataweb Can Support Cloud Federation: Service Representation and Secure Data Exchange. 2012 Second Symposium on Network Cloud Computing and Applications, 73–79. https://doi.org/10.1109/NCCA.2012.26

Cerroni, W. (2015). Network performance of multiple virtual machine live migration in cloud federations. Journal of Internet Services and Applications. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84926332621&doi=10.1186%2fs13174-015-0020-x&partnerID=40&md5=89cea1b1294ed052c81b6654d0921166

Chaimaa, B., Najib, E., & Rachid, H. (2017). A secure authentication model for Cloud federation. *INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND NETWORK SECURITY*, *17*(10), 89–94.

Challagidad, P. S., & Birje, M. N. (2020). Multi-dimensional dynamic trust evaluation scheme for cloud environment. *Computers & Security*, *91*, 101722. https://doi.org/10.1016/j.cose.2020.101722

Chen, H., An, B., Niyato, D., Soh, Y. C., & Miao, C. (2017). Workload Factoring and Resource Sharing via Joint Vertical and Horizontal Cloud Federation Networks. *IEEE Journal on Selected Areas in Communications*. Scopus.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85018916521&doi=10.1109%2fJSAC.2017.2659498&partnerID=40&md5=e0e1bd748417037aca09e03fe7b956d0

Comi, A., & Fotia, L. (2018). 39. Combining reliability, reputation and honesty to enhance QoS on federated computing infrastructures. *CEUR Workshop Proceedings*. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054307011&partnerID=40&md5=8b0cea41a8cdd2949b4b6784d29b328f

Comi, A., Fotia, L., Messina, F., Rosaci, D., & Sarné, G. M. L. (2016b). A partnership-based approach to improve QoS on federated computing infrastructures. *Information Sciences*, *367–368*, 246–258. https://doi.org/10.1016/j.ins.2016.05.051

Constine, J. (2012, November 13). Dropbox Is Now The Data Fabric Tying Together Devices For 100M Registered Users Who Save 1B Files A Day. *TechCrunch*. https://techcrunch.com/2012/11/13/dropbox-100-million/

Coronado, J. P. R., & Altmann, J. (2017). Model for incentivizing cloud service federation. International Conference on the Economics of Grids, Clouds, Systems, and Services, 233–246.

Czipura, C., & Jolly, D. R. (2007). Global airline alliances: Sparking profitability for a troubled industry. Journal of Business Strategy, 28(2), 57–64. https://doi.org/10.1108/02756660710732666

Darzanos, G., Koutsopoulos, I., & Stamoulis, G. D. (2015). A model for evaluating the economics of cloud federation. *2015 IEEE 4th International Conference on Cloud Networking (CloudNet)*, 291–296.

Darzanos, G., Koutsopoulos, I., & Stamoulis, G. D. (2016b). Economics models and policies for cloud federations. *2016 IFIP Networking Conference (IFIP Networking) and Workshops, IFIP Networking 2016*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84982292007&doi=10.1109%2fIFIPNetworking.2016.7497246&partnerID=40&md5=71f6bd2cd7de48d176c0fbe2a69ec8b3

Darzanos, G., Koutsopoulos, I., & Stamoulis, G. D. (2019b). Cloud federations: Economics, games and benefits. *IEEE/ACM Transactions on Networking*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85074866095&doi=10.1109%2fTNET.2019.2943810&partnerID=40&md5=d0555bb730fde5ed55f2c61713f61d3c

Das, A. K. (2015). *A QoS and Profit Aware Local and Global Cloud*

Confederation Model [PhD Thesis]. University of Dhaka.

Das, A. K., Adhikary, T., Razzaque, Md. A., Cho, E. J., & Hong, C. S. (2014). A QoS and profit aware cloud confederation model for IaaS service providers. *Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication, ICUIMC 2014*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84899752998&doi=10.1145%2f2557977.2558064&partnerID=40&md5=cede76f2d425882d2c8253864c2ebd65

Dhanabagyam, S. N., & Karpagam, G. R. (2018). Identity and access management as a service in e-healthcare cloud. *International Journal of Biomedical Engineering and Technology*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85042941276&doi=10.1504%2fIJBET.2018.089955&partnerID=40&md5=86f3c9c5aa93de4c96f80f451954b3aa

Dhole, A., Thomas, M. V., & Chandrasekaran, K. (2016b). An efficient trust-based Game-Theoretic approach for cloud federation formation. *2016 3rd International Conference on Advanced Computing and Communication Systems (ICACCS)*, *1*, 1–6.

Dinachali, B. P., Jabbehdari, S., & Javadi, H. H. S. (2022). 60. A cost-aware approach for cloud federation formation. *Transactions on*

Emerging Telecommunications Technologies. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85136992886&doi=10.1002%2fett.4631&partnerID=40&md5=9ee714350d22893ab948ab0943646ef2

Dodourova, M. (2009). Alliances as strategic tools: A cross-industry study of partnership planning, formation and success. *Management Decision*, *47*(5), 831–844. https://doi.org/10.1108/00251740910960150

Duan, Q. (2017). Cloud service performance evaluation: Status, challenges, and opportunities – a survey from the system modeling perspective. *Digital Communications and Networks*, *3*(2), 101–111. https://doi.org/10.1016/j.dcan.2016.12.002

Elmroth, E., Márquez, F. G., Henriksson, D., & Ferrera, D. P. (2009). Accounting and billing for federated cloud infrastructures. *8th International Conference on Grid and Cooperative Computing, GCC 2009*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-72349094320&doi=10.1109%2fGCC.2009.37&partnerID=40&md5=d82e4d51658441ebad87876292ed96b3

Elmuti, D., & Kathawala, Y. (2001). An overview of strategic alliances. *Management Decision*, *39*(3), 205–218.

https://doi.org/10.1108/EUM0000000005452

Emeakaroha, V. C., Healy, P., & Morrison, J. P. (2017). Facilitating Cloud Federation Management via Data Interoperability. In *Cloud Computing* (pp. 227–253). Springer.

Entrialgo, J., García, M., Díaz, J. L., García, J., & García, D. F. (2021). Modelling and simulation for cost optimization and performance analysis of transactional applications in hybrid clouds. Simulation Modelling Practice and Theory, 109, 102311. https://doi.org/10.1016/j.simpat.2021.102311

Evwiekpaefe, A. E., & Ajakaiye, F. (2013). The Trend and Challenges of Cloud Computing: A Literature Review. *Academic Journal of Interdisciplinary Studies*. https://doi.org/10.5901/ajis.2013.v2n10p9

Fan, C.-T., Chang, Y.-S., & Yuan, S.-M. (2018). VM instance selection for deadline constraint job on agent-based interconnected cloud. *Future Generation Computer Systems*, *87*, 470–487. https://doi.org/10.1016/j.future.2018.04.017

Farris, I., Militano, L., Nitti, M., Atzori, L., & Iera, A. (2017a). 25. MIFaaS: A Mobile-IoT-Federation-as-a-Service Model for dynamic cooperation of IoT Cloud Providers. *Future Generation*

Computer Systems, *70*, 126–137. https://doi.org/10.1016/j.future.2016.06.028

Farris, I., Militano, L., Nitti, M., Atzori, L., & Iera, A. (2017b). MIFaaS: A Mobile-IoT-Federation-as-a-Service Model for dynamic cooperation of IoT Cloud Providers. *Future Generation Computer Systems*, *70*, 126–137. https://doi.org/10.1016/j.future.2016.06.028

Feng, J., Yang, L. T., Zhu, Q., & Choo, K.-K. R. (2020). Privacy-preserving tensor decomposition over encrypted data in a federated cloud environment. IEEE Transactions on Dependable and Secure Computing. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85056602689&doi=10.1109%2fTDSC.2018.2881452&partnerID=40&md5=40e6caf5b965e90e28051911f2faadc2

Gardner, R., Campana, S., Duckeck, G., Elmsheuser, J., Hanushevsky, A., Hönig, F. G., Iven, J., Legger, F., Vukotic, I., Yang, W., & Collaboration, the A. (2014). Data federation strategies for ATLAS using XRootD. Journal of Physics: Conference Series, 513(4), 042049. https://doi.org/10.1088/1742-6596/513/4/042049

Gebrealif, Y., Mubarkoot, M., Altmann, J., & Egger, B. (2020). AI-Based Container Orchestration for Federated Cloud Environments.

Proceedings of the 1st Workshop on Flexible Resource and Application Management on the Edge, 15–16. https://doi.org/10.1145/3452369.3463818

Gebrealif, Y., Mubarkoot, M., Altmann, J., & Egger, B. (2021). Architecture for Orchestrating Containers in Cloud Federations. In K. Tserpes, J. Altmann, J. Á. Bañares, O. Agmon Ben-Yehuda, K. Djemame, V. Stankovski, & B. Tuffin (Eds.), *Economics of Grids, Clouds, Systems, and Services* (Vol. 13072, pp. 66–75). Springer International Publishing. https://doi.org/10.1007/978-3-030-92916-9_6

Gemser, G., Brand, M., & Sorge, A. (2012). Internationalisation strategies of technology-driven small- and medium-sized enterprises. Technology Analysis & Strategic Management, 24(3), 311–326. https://doi.org/10.1080/09537325.2012.655418

Ghenai, A., & Nouioua, C. (2020). Federation-Level Agreement and Integrity-Based Managed Cloud Federation Architecture. *Journal of Information Technology Research*, *13*, 91–117. https://doi.org/10.4018/JITR.2020100107

Giacobbe, M., Celesti, A., Fazio, M., Villari, M., & Puliafito, A. (2015). Evaluating a cloud federation ecosystem to reduce carbon footprint by moving computational resources. *2015 IEEE Symposium on*

Computers and Communication (ISCC), 99–104. https://doi.org/10.1109/ISCC.2015.7405500

Goiri, I., Guitart, J., & Torres, J. (2010). Characterizing Cloud Federation for Enhancing Providers' Profit. *2010 IEEE 3rd International Conference on Cloud Computing*, 123–130. https://doi.org/10.1109/CLOUD.2010.32

Goiri, Í., Guitart, J., & Torres, J. (2012). Economic model of a Cloud provider operating in a federated Cloud. *Information Systems Frontiers*, *14*(4), 827–843. https://doi.org/10.1007/s10796-011-9325-x

Gorjian Mehlabani, E., & Zhang, C. (2023). Improving virtualization and migration in combinatorial dynamic mapping for cloud services. *Cluster Computing*, *26*(2), 1511–1533. https://doi.org/10.1007/s10586-022-03720-1

Göv, S. A. (2020). Strategic Alliances in Airline Business: Comparision of Skyteam, Oneworld, Star Alliance Groups. Yönetim Bilimleri Dergisi, 18(38), Article 38. https://doi.org/10.35408/comuybd.629382

Govil, S. B., Thyagarajan, K., Srinivasan, K., Chaurasiya, V. K., & Das, S. (2012). An approach to identify the optimal cloud in cloud

federation. *International Journal of Cloud Computing and Services Science*, *1*(1), 35.

Grozev, N., & Buyya, R. (2014). Inter-Cloud architectures and application brokering: Taxonomy and survey. *Software: Practice and Experience*, *44*(3), 369–390. https://doi.org/10.1002/spe.2168

Gu, Z., Corcoglioniti, F., Lanti, D., Mosca, A., Xiao, G., Xiong, J., & Calvanese, D. (2022). A systematic overview of data federation systems. Semantic Web, Preprint(Preprint), 1–59. https://doi.org/10.3233/SW-223201

Guosun Zeng, Huanliang Xiong, Chunling Ding, Guijuan Kuang & Canghai Wu. (2022) Game strategies among multiple cloud computing platforms for non-cooperative competing assignment user tasks. The Journal of Supercomputing (2022) 78:14317–14342, https://doi.org/10.1007/s11227-022-04437-z,

Gupta, M. K., & Annappa, B. (2016). Trusted partner selection in broker based cloud federation. *2016 International Conference on Next Generation Intelligent Systems (ICNGIS)*, 1–6.

Hadjres, S., Belqasmi, F., El Barachi, M., & Kara, N. (2020a). 58. A green, energy, and trust-aware multi-objective cloud coalition formation approach. *Future Generation Computer Systems*, *111*,

52–67.

Hadjres, S., Kara, N., Barachi, M. E., & Belqasmi, F. (2021). An SLA-aware cloud coalition formation approach for virtualized networks. *IEEE Transactions on Cloud Computing*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85051798746&doi=10.1109%2fTCC.2018.2865737&partnerID=40&md5=1e730b36ff1674c9f83090c70676b952

Haile, N., & Altmann, J. (2015). *Risk-Benefit-Mediated Impact of Determinants on the Adoption of Cloud Federation*. Seoul National University; Technology Management, Economics, and Policy ….

Haile, N., & Altmann, J. (2018). Evaluating investments in portability and interoperability between software service platforms. *Future Generation Computer Systems*, *78*, 224–241. https://doi.org/10.1016/j.future.2017.04.040

Halabi, T. (2018). *Security in Cloud Computing: Evaluation and Integration* [PhD Thesis]. Ecole Polytechnique, Montreal (Canada).

Halabi, T., & Bellaiche, M. (2017). Service assignment in federated cloud environments based on multi-objective optimization of

security. *2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud)*, 39–46.

Halabi, T., & Bellaiche, M. (2020). 6. Towards Security-Based Formation of Cloud Federations: A Game Theoretical Approach. *IEEE Transactions on Cloud Computing*. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85044715791&doi=10.1109%2fTCC.2018.2820715&partnerID=40&md5=b5a1dbc64e823e48da03deb1cd232eb1

Halabi, T., Bellaiche, M., & Abusitta, A. (2018). A cooperative game for online cloud federation formation based on security risk assessment. *2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, 83–88.

Hammoud, A., Mourad, A., Otrok, H., Wahab, O. A., & Harmanani, H. (2020a). 42. Cloud federation formation using genetic and evolutionary game theoretical models. *Future Generation Computer Systems*, *104*, 92–104.

Hammoud, A., Mourad, A., Otrok, H., Wahab, O. A., & Harmanani, H. (2020b). Cloud federation formation using genetic and evolutionary game theoretical models. *Future Generation*

Computer Systems, *104*, 92–104.

Hammoud, A., Otrok, H., Mourad, A., Wahab, O. A., & Bentahar, J. (2018a). 21. On the detection of passive malicious providers in cloud federations. *IEEE Communications Letters*, *23*(1), 64–67.

Hammoud, A., Otrok, H., Mourad, A., Wahab, O. A., & Bentahar, J. (2018b). On the detection of passive malicious providers in cloud federations. *IEEE Communications Letters*, *23*(1), 64–67.

Hassan, M. M., Al-Wadud, M. A., & Fortino, G. (2015). A socially optimal resource and revenue sharing mechanism in cloud federations. 2015 IEEE 19th International Conference on Computer Supported Cooperative Work in Design (CSCWD), 620–625.

Hassan, M. M., Abdullah-Al-Wadud, M., Almogren, A., Rahman, S. M. M., Alelaiwi, A., Alamri, A., & Hamid, M. A. (2016a). 18. QoS and trust-aware coalition formation game in data-intensive cloud federations. *Concurrency and Computation: Practice and Experience*, *28*(10), 2889–2905.

Hassan, M. M., Abdullah-Al-Wadud, M., Almogren, A., Rahman, S. M. M., Alelaiwi, A., Alamri, A., & Hamid, M. A. (2016b). QoS and trust-aware coalition formation game in data-intensive cloud

federations. *Concurrency and Computation: Practice and Experience*, *28*(10), 2889–2905.

Hassan, M. M., Hossain, M. S., Sarkar, A. M., & Huh, E.-N. (2014a). Cooperative game-based distributed resource allocation in horizontal dynamic cloud federation platform. *Information Systems Frontiers*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84914684710&doi=10.1007%2fs10796-012-9357-x&partnerID=40&md5=8ec008cc912a1621e93af466fa6190c5

Hassan, M. M., Song, B., & Huh, E.-N. (2011). *Game-based distributed resource allocation in horizontal dynamic cloud federation platform*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-80455144664&doi=10.1007%2f978-3-642-24650-0_17&partnerID=40&md5=9dff9967b5a8b78119fc9d3f724252ba

Hassan, M. M., Song, B., Jehad Sarkar, A. M., & Huh, E.-N. (2012). Distributed resource allocation games in horizontal dynamic cloud federation platform. *Information*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84860202784&partnerID=40&md5=5a4a548cf6a1158e3a8d5f18

f5b8a9b7

Hayes, B. (2008). Cloud computing. *Communications of the ACM*, *51*(7), 9–11. https://doi.org/10.1145/1364782.1364786

Hosseinnezhad, M., Azgomi, M. A., & Dishabi, M. R. E. (2021). *A Probabilistic Trust Model for Cloud Services Using Bayesian Networks* [Preprint]. In Review. https://doi.org/10.21203/rs.3.rs-281906/v1

Hussain, W., Hussain, F. K., & Hussain, O. K. (2016). SLA Management Framework to Avoid Violation in Cloud. In A. Hirose, S. Ozawa, K. Doya, K. Ikeda, M. Lee, & D. Liu (Eds.), *Neural Information Processing* (pp. 309–316). Springer International Publishing. https://doi.org/10.1007/978-3-319-46675-0_34

IBM. (2011, April 7). *IBM Unveils Smart Cloud Services and Technologies for the Enterprise*. https://www.prnewswire.com/news-releases/ibm-unveils-smart-cloud-services-and-technologies-for-the-enterprise-119388729.html

Inc, G. (n.d.). SS&C Blue Prism Reviews, Ratings & Features 2023 | Gartner Peer Insights. Gartner. Retrieved May 20, 2023, from https://www.gartner.com/market/cloud-infrastructure-and-

platform-services/vendor/ssc-blue-prism/product/ss-and-c-blue-prism-enterprise

Jamba, B., & Aluvalu, R. (2016). *Interoperability in Cloud Federation: A Survey Interoperability in Cloud Federation: A Survey*. *January 2015*.

Javed, A., Robert, J., Heljanko, K., & Främling, K. (2020). IoTEF: A Federated Edge-Cloud Architecture for Fault-Tolerant IoT Applications. *Journal of Grid Computing*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85077679245&doi=10.1007%2fs10723-019-09498-8&partnerID=40&md5=df91627c6d21243cef19c4cab7e9a1e3

Jones, S., Irani, Z., Sivarajah, U., & Love, P. E. D. (2019). Risks and rewards of cloud computing in the UK public sector: A reflection on three Organisational case studies. *Information Systems Frontiers*, *21*(2), 359–382. https://doi.org/10.1007/s10796-017-9756-0

Joshi, M., Pal, A., & Sankarasubbu, M. (2022). Federated Learning for Healthcare Domain—Pipeline, Applications and Challenges. ACM Transactions on Computing for Healthcare, 3(4), 40:1-40:36. https://doi.org/10.1145/3533708

Kamalian, A., Hemmat, Z., & Jolfaie, S. A. D. (2015). Cooperation Networks and Innovation Performance of Small and Medium-Sized Enterprises (SMEs). https://www.semanticscholar.org/paper/Cooperation-Networks-and-Innovation-Performance-of-Kamalian-Hemmat/acde4c8d2ad5f352d4121d6050127f11013943ba

Kanwal, A., Masood, R., & Shibli, M. A. (2014). Evaluation and establishment of trust in cloud federation. *Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication, ICUIMC 2014*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84899760598&doi=10.1145%2f2557977.2558023&partnerID=40&md5=37391e418deea959a3235e24dcd1ad10

Kathryn North, A. M. (2015). The global alliance for genomics and health: Towards international sharing of genomic and clinical data. Pathology, 47, S28–S29. https://doi.org/10.1097/01.PAT.0000461407.88852.73

Kertesz, A. (2014). Characterizing Cloud Federation Approaches. In Z. Mahmood (Ed.), *Cloud Computing* (pp. 277–296). Springer International Publishing. https://doi.org/10.1007/978-3-319-10530-7_12

Kertesz, A., & Varadi, S. (2014). Legal Aspects of Data Protection in Cloud Federations. In S. Nepal & M. Pathan (Eds.), *Security, Privacy and Trust in Cloud Systems* (pp. 433–455). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-38586-5_15

Khan, K. M., & Malluhi, Q. (2010). Establishing Trust in Cloud Computing. *IT Professional*, *12*(5), 20–27. https://doi.org/10.1109/MITP.2010.128

Khandelwal, Y., Dogra, A., Ganti, K., Purini, S., & Reddy, P. V. (2021). Pricing strategies of an oligopolist in federated cloud markets. Journal of Cloud Computing, 10(1), 1–13.

Khandelwal, Y., Ganti, K., Purini, S., & Reddy, P., V. (2018). 43. Cloud Federation Formation in Oligopolistic Markets. In M. Aldinucci, L. Padovani, & M. Torquati (Eds.), *EURO-PAR 2018: PARALLEL PROCESSING* (Vol. 11014, pp. 392–403). Univ Turin, Comp Sci Dept. https://doi.org/10.1007/978-3-319-96983-1_28

Khandelwal, Y., Purini, S., & Reddy, P. V. (2016). Fast algorithms for optimal coalition formation in federated clouds. *2016 IEEE/ACM 9th International Conference on Utility and Cloud Computing (UCC)*, 156–164.

Kholod, I., Yanaki, E., Fomichev, D., Shalugin, E., Novikova, E.,

Filippov, E., & Nordlund, M. (2021). Open-Source Federated Learning Frameworks for IoT: A Comparative Review and Analysis. Sensors, 21(1), Article 1. https://doi.org/10.3390/s21010167

Khorasani, N., Abrishami, S., Feizi, M., Esfahani, M. A., & Ramezani, F. (2020). 59. Resource management in the federated cloud environment using Cournot and Bertrand competitions. *Future Generation Computer Systems*, *113*, 391–406. https://doi.org/10.1016/j.future.2020.07.010

Khorshed, M. T., Ali, A. B. M. S., & Wasimi, S. A. (2011). Trust Issues that Create Threats for Cyber Attacks in Cloud Computing. *2011 IEEE 17th International Conference on Parallel and Distributed Systems*, 900–905. https://doi.org/10.1109/ICPADS.2011.156

Kim, D., Muhammad, H., Kim, E., Helal, S., & Lee, C. (2019). TOSCA-based and federation-aware cloud orchestration for Kubernetes container platform. Applied Sciences (Switzerland). Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85059637483&doi=10.3390%2fapp9010191&partnerID=40&md5=c374f057c27f4449fa98acd3d7d2f2ba

Kim, K., Kang, S., & Altmann, J. (2014). Cloud Goliath Versus a Federation of Cloud Davids. In J. Altmann, K. Vanmechelen, & O.

F. Rana (Eds.), *Economics of Grids, Clouds, Systems, and Services* (pp. 55–66). Springer International Publishing. https://doi.org/10.1007/978-3-319-14609-6_4

Kirthica, S., & Sridhar, R. (2018). 11. Securely communicating with an optimal cloud for intelligently enhancing a cloud's elasticity. *International Journal of Intelligent Information Technologies*. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85047727474&doi=10.4018%2fIJIIT.2018040103&partnerID=40&md5=37b1bb5cbd59c61b8b3f9dbe3223b3c5

Kitchenham, B. A., Budgen, D., & Brereton, P. (2015). *Evidence-Based Software Engineering and Systematic Reviews*. CRC Press.

Knepper, R., Mehringer, S., Brazier, A., Barker, B., & Reynolds, R. (2019). Red Cloud and Aristotle: Campus clouds and federations. Proceedings of the Humans in the Loop: Enabling and Facilitating Research on Cloud Computing, 1–6. https://doi.org/10.1145/3355738.3355755

Kollolu, R. (2020). History, Deployment and Service Models Towards the Evolution of Cloud Computing. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3917250

Kousiouris, G., Vafiadis, G., & Corrales, M. (2013). *A Cloud provider*

description schema for meeting legal requirements in Cloud federation scenarios. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84882939768&doi=10.1007%2f978-3-642-37437-1_6&partnerID=40&md5=d1bcf5f0becae096b080fff4cca5c096

Kurze, T., Klems, M., Bermbach, D., Lenk, A., Tai, S., & Kunze, M. (2011). Cloud Federation. *Computing*, 7. https://www.researchgate.net/publication/312280049_Cloud_federation

Lansing, J., & Sunyaev, A. (2016). Trust in Cloud Computing: Conceptual Typology and Trust-Building Antecedents. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *47*(2), 58–96. https://doi.org/10.1145/2963175.2963179

Larsson, L., Henriksson, D., & Elmroth, E. (2011). Scheduling and monitoring of internally structured services in cloud federations. *Proceedings - IEEE Symposium on Computers and Communications*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-80052742050&doi=10.1109%2fISCC.2011.5984012&partnerID=40&md5=474843da358ba1b2e7bf5d650adcefc2

Latif, R., Afzaal, S. H., & Latif, S. (2021). 57. A novel cloud

management framework for trust establishment and evaluation in a federated cloud environment. *Journal of Supercomputing*. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85104130905&doi=10.1007%2fs11227-021-03775-8&partnerID=40&md5=9352984d5a89e149390a2df92c88a34b

Latif, S., Humayun, M., Sharif, A., & Kadry, S. (2022). Resource discovery and scalability-aware routing in cloud federation using distributed meta-brokering paradigm. *International Journal of Web and Grid Services*, *18*(1), 34. https://doi.org/10.1504/IJWGS.2022.119269

Law, S. H., & Azman-Saini, W. N. W. (2012). Institutional quality, governance, and financial development. Economics of Governance, 13(3), 217–236. https://doi.org/10.1007/s10101-012-0112-z

Lee, C. A. (2016). Cloud Federation Management and Beyond: Requirements, Relevant Standards, and Gaps. *IEEE Cloud Computing*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84963738720&doi=10.1109%2fMCC.2016.15&partnerID=40&md5=657aa5ebf8dafbab68b3a471e58c9e7c

Licklider, J. C. R. (1963). *Intergalactic Computer Network*.

Li, K. (2021). On the profits of competing cloud service providers: A game theoretic approach. *Journal of Computer and System Sciences, 117*, 130–153. https://doi.org/10.1016/j.jcss.2020.10.008

Li, K. (2022). Profit Maximization in a Federated Cloud by Optimal Workload Management and Server Speed Setting. IEEE Transactions on Sustainable Computing. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85138466392&doi=10.1109%2fTSUSC.2021.3126666&partnerID=40&md5=a1af6b093d9cfe3775140913eff0a45e

Li, L., Fan, Y., Tse, M., & Lin, K.-Y. (2020). A review of applications in federated learning. Computers & Industrial Engineering, 149, 106854. https://doi.org/10.1016/j.cie.2020.106854

Li, L., Liu, L., Huang, S., Lv, S., Lin, K., & Zhu, S. (2022). Agent-based multi-tier SLA negotiation for intercloud. *Journal of Cloud Computing*, *11*(1), 16. https://doi.org/10.1186/s13677-022-00286-6

Li, Y., Dai, W., Gan, X., Jin, H., Fu, L., Ma, H., & Wang, X. (2022). Cooperative Service Placement and Scheduling in Edge Clouds: A Deadline-Driven Approach. *IEEE Transactions on Mobile Computing*. https://www.scopus.com/inward/record.uri?eid=2-

s2.0-85101742044&doi=10.1109%2fTMC.2021.3061602&partnerID=40&md5=9940e20a388b884ffa06e53be3b17c1d

Li, Y., Xia, M., Duan, J., & Chen, Y. (2022). Pricing-based resource allocation in three-tier edge computing for social welfare maximization. Computer Networks, 217, 109311. https://doi.org/10.1016/j.comnet.2022.109311

Licklider, J. C. R. (1963). *Intergalactic Computer Network*.

Lindpaintner, J. (2019, March 5). 18F: Digital service delivery | The U.S. Data Federation wants to make it easier to collect, combine, and exchange data across government. https://18f.gsa.gov/2019/03/05/the-us-data-federation/

Liu, L., Zhang, J., Song, S. H., & Letaief, K. (2019). Edge-Assisted Hierarchical Federated Learning with Non-IID Data. ArXiv. https://www.semanticscholar.org/paper/Edge-Assisted-Hierarchical-Federated-Learning-with-Liu-Zhang/85a72cc775cf621474643aac98d1a86ce7d49764

Liu, L., Zhang, J., Song, S. H., & Letaief, K. B. (2020). Client-Edge-Cloud Hierarchical Federated Learning. ICC 2020 - 2020 IEEE International Conference on Communications (ICC), 1–6.

https://doi.org/10.1109/ICC40277.2020.9148862

Liu, T., Di, B., An, P., & Song, L. (2021). Privacy-Preserving Incentive Mechanism Design for Federated Cloud-Edge Learning. IEEE Transactions on Network Science and Engineering, 8(3), 2588–2600. Scopus. https://doi.org/10.1109/TNSE.2021.3100096

López García, Á., Fernández del Castillo, E., & Orviz Fernández, P. (2016). Standards for enabling heterogeneous IaaS cloud federations. Computer Standards & Interfaces, 47, 19–23. https://doi.org/10.1016/j.csi.2016.02.002

Loubière, P., & Tomassetti, L. (2020). Towards Cloud Computing. In *TORUS 1 – Toward an Open Resource Using Services* (pp. 179–189). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781119720492.ch13

Maria Manuel Vianny, D., & Aramudhan, M. (2017). An efficient technique for trust based cloud providers ranking in federated cloud. *International Journal of Applied Engineering Research*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85057642778&partnerID=40&md5=e2bd220a17fc64f9b62ba5e7147256f5

Mary, Z. (2023, January 1). *Top 10 Cloud Service Providers Globally in*

2023—Dgtl Infra. https://dgtlinfra.com/top-10-cloud-service-providers-2022/

Mashayekhy, L., & Grosu, D. (2013). A merge-and-split mechanism for dynamic virtual organization formation in grids. *IEEE Transactions on Parallel and Distributed Systems*, *25*(3), 540–549.

Mashayekhy, L., Nejad, M. M., & Grosu, D. (2014). A framework for data protection in cloud federations. 2014 43rd International Conference on Parallel Processing, 283–290.

Mashayekhy, L., Nejad, M. M., & Grosu, D. (2021). A Trust-Aware Mechanism for Cloud Federation Formation. *IEEE Transactions on Cloud Computing*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85121056078&doi=10.1109%2fTCC.2019.2911831&partnerID=40&md5=e905a66252176204c339009b4624c034

Massonet, P., Levin, A., Celesti, A., & Villari, M. (2016). Security requirements in a federated cloud networking architecture. *Communications in Computer and Information Science*. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84966586562&doi=10.1007%2f978-3-319-33313-7_6&partnerID=40&md5=285801e8db2a7b55323e1d2f41dd13ea

Massonet, P., Naqvi, S., Ponsard, C., Latanicki, J., Rochwerger, B., & Villari, M. (2011). A monitoring and audit logging architecture for data location compliance in federated cloud infrastructures. *IEEE International Symposium on Parallel and Distributed Processing Workshops and Phd Forum*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-83455220824&doi=10.1109%2fIPDPS.2011.304&partnerID=40&md5=ccb1f0f6ea9ead82cbfa9f481473b8b1

Massonet, P., & Sheridan, C. (2016). BEACON – Enabling federated cloud networking. Communications in Computer and Information Science. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84966477948&partnerID=40&md5=e772c15f1d4f32d5b7a78f25bb38f0f8

Matthew Vulpis. (2023, January). *Cloud Services and Applications Will Continue to Grow in 2023: A Few Important Trends*. https://cloud-computing.tmcnet.com/breaking-news/articles/454745-cloud-services-applications-will-continue-grow-2023-few.htm

Mellaoui, W., Posso, R., Gebrealif, Y., Bock, E., Altmann, J., & Yoon, H. (2021). Knowledge Management Framework for Cloud Federation. In K. Tserpes, J. Altmann, J. Á. Bañares, O. Agmon Ben-Yehuda, K. Djemame, V. Stankovski, & B. Tuffin (Eds.),

Economics of Grids, Clouds, Systems, and Services (Vol. 13072, pp. 123–132). Springer International Publishing. https://doi.org/10.1007/978-3-030-92916-9_10

Meng, X., & Zhang, G. (2020). TrueTrust: A feedback-based trust management model without filtering feedbacks in P2P networks. Peer-to-Peer Networking and Applications, 13(1), 175–189. https://doi.org/10.1007/s12083-019-00742-2

Messina, F., Pappalardo, G., Comi, A., Fotia, L., Rosaci, D., & Sarné, G. M. L. (2017). Combining reputation and QoS measures to improve cloud service composition. *International Journal of Grid and Utility Computing*, *8*(2), 142. https://doi.org/10.1504/IJGUC.2017.085915

Messina, F., Pappalardo, G., & Santoro, C. (2014). Decentralised Resource Finding and Allocation in Cloud Federations. *2014 International Conference on Intelligent Networking and Collaborative Systems*, 26–33. https://doi.org/10.1109/INCoS.2014.70

Messina, F., Pappalardo, G., Santoro, C., Rosaci, D., & Sarné, G. M. L. (2016). A multi-agent protocol for service level agreement negotiation in cloud federations. *International Journal of Grid and Utility Computing*, *7*(2), 101.

https://doi.org/10.1504/IJGUC.2016.077488

Moghaddam, M. M., Manshaei, M. H., Soorki, M. N., Saad, W., Goudarzi, M., & Niyato, D. (2020a). 22. On Coordination of Smart Grid and Cooperative Cloud Providers. *IEEE Systems Journal*, *15*(1), 672–683.

Moghaddam, M. M., Manshaei, M. H., Soorki, M. N., Saad, W., Goudarzi, M., & Niyato, D. (2020b). On Coordination of Smart Grid and Cooperative Cloud Providers. *IEEE Systems Journal*, *15*(1), 672–683.

Mohamad, M. R. B. (2012). Competitive strategy of Malaysian small and medium enterprises: An exploratory investigation. https://www.semanticscholar.org/paper/Competitive-strategy-of-Malaysian-small-and-medium-Mohamad/a776ffef12c635732b66f9e7037cf1eeed72b163

Moreno-Vozmediano, R., Huedo, E., Llorente, I. M., Montero, R. S., Massonet, P., Villari, M., Merlino, G., Celesti, A., Levin, A., Schour, L., Vazquez, C., Melis, J., Spahr, S., & Whigham, D. (2016). BEACON: A Cloud Network Federation Framework. In A. Celesti & P. Leitner (Eds.), ADVANCES IN SERVICE-ORIENTED AND CLOUD COMPUTING (ESOCC 2015) (Vol. 567, pp. 325–337). IFIP; Univ Messina, Mobile & Distributed Syst

Lab; Univ Messina, Dept Engn. https://doi.org/10.1007/978-3-319-33313-7_25

Moreno-Vozmediano, R., Huedo, E., Llorente, I. M., Montero, R. S., Massonet, P., Villari, M., Merlino, G., Celesti, A., Levin, A., Schour, L., Vázquez, C., Melis, J., Spahr, S., & Whigham, D. (2016). BEACON: A cloud network federation framework. Communications in Computer and Information Science. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84966687575&doi=10.1007%2f978-3-319-33313-7_25&partnerID=40&md5=b9151e00d686a6cefbe7a054e95dad57

Moreno-Vozmediano, R., Montero, R. S., Huedo, E., & Llorente, I. M. (2017). Implementation and Provisioning of Federated Networks in Hybrid Clouds. *Journal of Grid Computing*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85015891804&doi=10.1007%2fs10723-017-9395-1&partnerID=40&md5=323dd178b42509d8237c43427cc189b2

Mourougan, S., & Aramudhan, M. (2016a). Regression tree based ranking model in federated cloud. *Indian Journal of Science and Technology*. https://www.scopus.com/inward/record.uri?eid=2-s2.0-

84977555802&doi=10.17485%2fijst%2f2016%2fv9i22%2f95279&partnerID=40&md5=22dc02c20a2b7865090f158f06d4db51

Mowla, M. M. (2012). An Overview of Strategic Alliance: Competitive Advantages in Alliance Constellations. *Advances in Management*, *5*(12). https://typeset.io/papers/an-overview-of-strategic-alliance-competitive-advantages-in-34kskf5oxi

Mujawar, T. N., & Bhajantri, L. B. (2022). Behavior and feedback based trust computation in cloud environment. Journal of King Saud University - Computer and Information Sciences, 34(8, Part A), 4956–4967. https://doi.org/10.1016/j.jksuci.2020.12.003

Muralidharan, C., & Anitha, R. (2022). Trusted cloud broker for estimating the reputation of cloud providers in federated cloud environment. *Concurrency and Computation: Practice and Experience*, *34*(1). https://doi.org/10.1002/cpe.6537

Muthu, M. (2016). Cloud Computing: A Play for Vital Role in Libraries. *Pearl : A Journal of Library and Information Science*, *10*(4), 281. https://doi.org/10.5958/0975-6922.2016.00039.5

Najm, M., & Tamarapalli, V. (2022). Towards cost-aware VM migration to maximize the profit in federated clouds. *Future Generation Computer Systems*, *134*, 53–65.

https://doi.org/10.1016/j.future.2022.03.020

Nawaz, F., Hussain, O., Hussain, F. K., Janjua, N. K., Saberi, M., & Chang, E. (2019). Proactive management of SLA violations by capturing relevant external events in a Cloud of Things environment. *Future Generation Computer Systems*, *95*, 26–44. https://doi.org/10.1016/j.future.2018.12.034

Nazareth, D. L., & Choi, J. (2021). Market Share Strategies for Cloud Computing Providers. Journal of Computer Information Systems, 61(2), 182–192. https://doi.org/10.1080/08874417.2019.1576022

Nemati, H., El Barachi, M., Kara, N., & Belqasmi, F. (2019a). 56. A novel game theoretic approach for forming coalitions between IMS cloud providers. *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, 1–7.

Nemati, H., El Barachi, M., Kara, N., & Belqasmi, F. (2019b). A novel game theoretic approach for forming coalitions between IMS cloud providers. *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, 1–7.

Ng, D., Lan, X., Yao, M. M.-S., Chan, W. P., & Feng, M. (2021). Federated learning: A collaborative effort to achieve better medical imaging models for individual sites that have small labelled

datasets. Quantitative Imaging in Medicine and Surgery, 11(2), 852–857. https://doi.org/10.21037/qims-20-595

Nocentino, A. E., & Weissman, B. (2021). Azure Arc–Enabled Data Services and High Availability for SQL Server on Kubernetes. In A. E. Nocentino & B. Weissman (Eds.), *SQL Server on Kubernetes: Designing and Building a Modern Data Platform* (pp. 197–214). Apress. https://doi.org/10.1007/978-1-4842-7192-6_9

Noltes, J. (2011, August 26). *Data location compliance in cloud computing* [Info:eu-repo/semantics/masterThesis]. University of Twente. https://essay.utwente.nl/61042/

Nugraha, Y., & Martin, A. (2021). Towards a framework for trustworthy data security level agreement in cloud procurement. *Computers & Security*, *106*, 102266. https://doi.org/10.1016/j.cose.2021.102266

Obasuyi, G. C., & Sari, A. (2015). Security Challenges of Virtualization Hypervisors in Virtualized Hardware Environment. *International Journal of Communications, Network and System Sciences*, *08*(07), Article 07. https://doi.org/10.4236/ijcns.2015.87026

Okoli, C. (2015). A Guide to Conducting a Standalone Systematic Literature Review. *Communications of the Association for Information Systems*, *37*(1).

https://doi.org/10.17705/1CAIS.03743

Opara-Martins, J., Sahandi, R., & Tian, F. (2016). Critical analysis of vendor lock-in and its impact on cloud computing migration: A business perspective. Journal of Cloud Computing, 5(1), 4. https://doi.org/10.1186/s13677-016-0054-z

Organizing Successful Co-Marketing Alliances—Louis P. Bucklin, Sanjit Sengupta, 1993. (n.d.). Retrieved April 25, 2023, from https://journals.sagepub.com/doi/10.1177/002224299305700203

Pacini, E., Iacono, L., Mateos, C., & García Garino, C. (2019). 62. A Bio-inspired Datacenter Selection Scheduler for Federated Clouds and Its Application to Frost Prediction. *Journal of Network and Systems Management*. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85057128631&doi=10.1007%2fs10922-018-9481-0&partnerID=40&md5=8e53be5cd9070f08d48e6d1981e0b787

Pal, R., Lin, S.-H., Ahujay, A., & Golubchik, L. (2017). *The Cloudlet Bazaar Dynamic Markets for the Small Cloud*. https://doi.org/10.48550/ARXIV.1704.00845

Panarello, A., Celesti, A., Fazio, M., Puliafito, A., & Villari, M. (2016). A Federated System for MapReduce-Based Video Transcoding to

Face the Future Massive Video-Selfie Sharing Trend. In A. Celesti & P. Leitner (Eds.), *ADVANCES IN SERVICE-ORIENTED AND CLOUD COMPUTING (ESOCC 2015)* (Vol. 567, pp. 48–62). IFIP; Univ Messina, Mobile & Distributed Syst Lab; Univ Messina, Dept Engn. https://doi.org/10.1007/978-3-319-33313-7_4

Panarello, A., Celesti, A., Fazio, M., Villari, M., & Puliafito, A. (2014). A requirements analysis for IaaS cloud federation. *CLOSER 2014 - Proceedings of the 4th International Conference on Cloud Computing and Services Science*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84902319762&doi=10.5220%2f0004945705840589&partnerID=40&md5=715eddf03d5dbdacf24574f05d3c3293

Papadakis-Vlachopapadopoulos, K., González, R. S., Dimolitsas, I., Dechouniotis, D., Ferrer, A. J., & Papavassiliou, S. (2019). Collaborative SLA and reputation-based trust management in cloud federations. *Future Generation Computer Systems*, *100*, 498–512. https://doi.org/10.1016/j.future.2019.05.030

Patel, A. A. (2018). Cloud Computing: Amazon Web Services (Infrastructure on Demand). *International Journal for Research in Applied Science and Engineering Technology*, *6*(6), 1410–1415. https://doi.org/10.22214/ijraset.2018.6206

Pearson, S., & Benameur, A. (2010). Privacy, Security and Trust Issues Arising from Cloud Computing. *2010 IEEE Second International Conference on Cloud Computing Technology and Science*, 693–702. https://doi.org/10.1109/CloudCom.2010.66

Petrescu, R. V. V., Aversa, R., Akash, B., Corchado, J. M., Apicella, A., & Petrescu, F. I. T. (2017). Home at Airbus. Journal of Aircraft and Spacecraft Technology, 1(2), 97–118. https://doi.org/10.3844/jastsp.2017.97.118

Petri, I., Beach, T., Rana, O. F., & Rezgui, Y. (2017). Coordinating multi-site construction projects using federated clouds. Automation in Construction, 83, 273–284. https://doi.org/10.1016/j.autcon.2017.08.011

Petri, I., Rana, O., Beach, T., Rezgui, Y., & Sutton, A. (2015). Clouds4Coordination: Managing Project Collaboration in Federated Clouds. *Proceedings - 2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing, UCC 2015*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84965011021&doi=10.1109%2fUCC.2015.88&partnerID=40&md5=c16f3562da553a91904a7f9acab1b055

Petri, I., Zou, M., Zamani, A. R., Diaz-Montes, J., Rana, O., & Parashar,

M. (2015). Integrating Software Defined Networks within a Cloud Federation. *2015 15th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, 179–188. https://doi.org/10.1109/CCGrid.2015.11

Phani Krishna Kollapur Gandla. (2023, February). *Hybrid and Federated Cloud Computing—DZone*. Dzone.Com. https://dzone.com/articles/common-hybrid-cloud-federation-models

Piroozi, F., Romão, M. J. B., Costa, C. J., & Aparicio, M. (2021). A literature review to determine the critical success factors during different phases of strategic alliance lifecycle [Uma revisão da literatura para determinar os fatores críticos de sucesso durante as diferentes fases do ciclo de vida da aliança estratégica]. *Internatinal Symposium on Management, Project, Innovation and Sustainability*, 1–8.

Pradeep Kumar, V., & Prakash, K. B. (2019). QoS aware resource provisioning in federated cloud and analyzing maximum resource utilization in agent based model. *International Journal of Innovative Technology and Exploring Engineering*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85067949396&partnerID=40&md5=c04ff53d283d715d9248170b

ea8d53c0

Qiu, B., & Gooi, H. B. (2000). Web-based SCADA display systems (WSDS) for access via Internet. *IEEE Transactions on Power Systems*, *15*(2), 681–686. https://doi.org/10.1109/59.867159

Quem Somos – Angola Cables. (n.d.). Retrieved May 20, 2023, from https://www.angolacables.co.ao/en/quem-somos/

Rahimzadeh, V., Dyke, S. O. M., & Knoppers, B. M. (2016). An International Framework for Data Sharing: Moving Forward with the Global Alliance for Genomics and Health. Biopreservation and Biobanking, 14(3), 256–259. https://doi.org/10.1089/bio.2016.0005

Ramezani, F., Abrishami, S., & Feizi, M. (2022). A Market-based Framework for Resource Management in Cloud Federation. *Journal of Grid Computing*, *21*(1), 3. https://doi.org/10.1007/s10723-022-09635-w

Ray, B. K., Saha, A., Khatua, S., & Roy, S. (2019). 8. Toward maximization of profit and quality of cloud federation: Solution to cloud federation formation problem. *The Journal of Supercomputing*, *75*(2), 885–929.

Ray, B. K., Saha, A., Khatua, S., & Roy, S. (2021a). 16. Quality and

Profit Assured Trusted Cloud Federation Formation: Game Theory Based Approach. *IEEE Transactions on Services Computing*. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85046784722&doi=10.1109%2fTSC.2018.2833854&partnerID=40&md5=b27e4e6ed1639591f66b8d35e2fba99a

Ray, B. K., Saha, A., Khatua, S., & Roy, S. (2021b). Quality and Profit Assured Trusted Cloud Federation Formation: Game Theory Based Approach. *IEEE Transactions on Services Computing*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85046784722&doi=10.1109%2fTSC.2018.2833854&partnerID=40&md5=b27e4e6ed1639591f66b8d35e2fba99a

Ray, B. K., Saha, A., & Roy, S. (2018). Migration cost and profit oriented cloud federation formation: Hedonic coalition game based approach. *Cluster Computing*, *21*(4), 1981–1999.

Rebai, S. (2017, March 13). Resource allocation in Cloud federation. https://www.semanticscholar.org/paper/Resource-allocation-in-Cloud-federation-Rebai/d831cf90fcd21053772277f20ff175f4ffed6128

Ries, S. (2007). Certain trust: A trust model for users and agents. *Proceedings of the 2007 ACM Symposium on Applied Computing - SAC '07*, 1599.

https://doi.org/10.1145/1244002.1244342

Ries, S. (2009). *Trust in Ubiquitous Computing* [Phd, Technische Universität]. https://tuprints.ulb.tu-darmstadt.de/1948/

Richardson, J., Sallam, R., Schlegel, K., Kronz, A., & Sun, J. (2020). Magic quadrant for analytics and business intelligence platforms. *Gartner ID G00386610*.

Robbins, B. G. (2012). Institutional Quality and Generalized Trust: A Nonrecursive Causal Model. Social Indicators Research, 107(2), 235–258. https://doi.org/10.1007/s11205-011-9838-1

Roche, K., & Douglas, J. (2009). Beginning Google App Engine for Java. In K. Roche & J. Douglas, *Beginning Java™ Google App Engine* (pp. 1–6). Apress. https://doi.org/10.1007/978-1-4302-2554-6_1

Rochwerger, B., Breitgand, D., Levy, E., Galis, A., Nagin, K., Llorente, I. M., Montero, R., Wolfsthal, Y., Elmroth, E., Cáceres, J., Ben-Yehuda, M., Emmerich, W., & Galán, F. (2009). The Reservoir model and architecture for open federated cloud computing. *IBM Journal of Research and Development*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-74049087607&doi=10.1147%2fJRD.2009.5429058&partnerID=40&md5=86c2ac77cea8c489f65d0410878115fb

Romero Coronado, J. P., & Altmann, J. (2017a). 23. Model for incentivizing cloud service federation. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85032482917&doi=10.1007%2f978-3-319-68066-8_18&partnerID=40&md5=615fdbddf64814dfbe3445960676535b

Romero Coronado, J. P., & Altmann, J. (2017b). *Model for incentivizing cloud service federation*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85032482917&doi=10.1007%2f978-3-319-68066-8_18&partnerID=40&md5=615fdbddf64814dfbe3445960676535b

Russo, M., & Cesarani, M. (2017). Strategic Alliance Success Factors: A Literature Review on Alliance Lifecycle. *International Journal of Business Administration*, *8*(3), 1. https://doi.org/10.5430/ijba.v8n3p1

Sajid, S., Jawad, M., Hamid, K., Khan, M. U. S., Ali, S. M., Abbas, A., & Khan, S. U. (2021). Blockchain-based decentralized workload and energy management of geo-distributed data centers.

Sustainable Computing: Informatics and Systems, 29, 100461. https://doi.org/10.1016/j.suscom.2020.100461

Samaan, N. (2014). A novel economic sharing model in a federation of selfish cloud providers. IEEE Transactions on Parallel and Distributed Systems. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84904563140&doi=10.1109%2fTPDS.2013.23&partnerID=40&md5=e3b17aa9d197adf985c345703e8e2b1f

Samlinson, E., & Usha, M. (2013). User-centric trust based identity as a service for federated cloud environment. *2013 4th International Conference on Computing, Communications and Networking Technologies, ICCCNT 2013*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84894422064&doi=10.1109%2fICCCNT.2013.6726636&partnerID=40&md5=0d61d6e17a68b7bf3363d493604fc4b3

Satheesh, M., & Aramudhan, M. (2019). Cloud ranking model for optimal service selection based on random fuzzy logic. *Journal of Theoretical and Applied Information Technology*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85065236829&partnerID=40&md5=0acbecd98f438fff6eadd553bfe5dd89

Saxena, D., Vaisla, K. S., & Rauthan, M. S. (2019). Abstract Model of Trusted and Secure Middleware Framework for Multi-cloud Environment. *Communications in Computer and Information Science*. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85058301872&doi=10.1007%2f978-981-13-3143-5_38&partnerID=40&md5=4e5261d1e8a88bc55be5a0ab85a8f567

Segrestin, B. (2005). Partnering to explore: The Renault–Nissan Alliance as a forerunner of new cooperative patterns. Research Policy, 34(5), 657–672. https://doi.org/10.1016/j.respol.2005.02.006

Shan, C., Heng, C., & Xianjun, Z. (2012). Inter-cloud operations via NGSON. *IEEE Communications Magazine*, *50*(1), 82–89. https://doi.org/10.1109/MCOM.2012.6122536

Shi, Z., Zhou, H., Laat, C. de, & Zhao, Z. (2022). A Bayesian game-enhanced auction model for federated cloud services using blockchain. *Future Generation Computer Systems*, *136*, 49–66. https://doi.org/10.1016/j.future.2022.05.017

Shrivastava, S., & Pateriya, R. K. (2020a). 35. Data encoding and cost optimised distribution for efficient and secure storage in cloud federation. *International Journal of Information and Computer Security*. https://www.scopus.com/inward/record.uri?eid=2-s2.0-

85092277135&doi=10.1504%2fIJICS.2020.109484&partnerID=40&md5=964d7d720bcb876ca38402412cd424b8

Shrivastava, S., & Pateriya, R. K. (2020b). Data encoding and cost optimised distribution for efficient and secure storage in cloud federation. *International Journal of Information and Computer Security*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85092277135&doi=10.1504%2fIJICS.2020.109484&partnerID=40&md5=964d7d720bcb876ca38402412cd424b8

Singh, S., & Sidhu, J. (2017). Compliance-based Multi-dimensional Trust Evaluation System for determining trustworthiness of Cloud Service Providers. *Future Generation Computer Systems*, *67*, 109–132. https://doi.org/10.1016/j.future.2016.07.013

Sitaram, D., Harwalkar, S., & Kumar, K. V. S. (2016). Standards Based Integration of Intercloud for Federation with OpenStack. 2016 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), 113–118. https://doi.org/10.1109/CCEM.2016.028

Song, S. (2017). Competition law and interoperability in cloud computing. Computer Law & Security Review, 33(5), 659–671. https://doi.org/10.1016/j.clsr.2017.05.005

Sotiriadis, S., Bessis, N., & Petrakis, E. G. M. (2014). *An inter-cloud architecture for future internet infrastructures*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84915821125&doi=10.1007%2f978-3-319-13464-2_15&partnerID=40&md5=981410c4d976922be016663a5af0207b

STAMFORD, Conn. (2023, April). *Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $600 Billion in 2023*. Gartner. https://www.gartner.com/en/newsroom/press-releases/2023-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023

Stergiou, C. L., Psannis, K. E., & Gupta, B. B. (2022). InFeMo: Flexible Big Data Management Through a Federated Cloud System. ACM Transactions on Internet Technology, 22(2). Scopus. https://doi.org/10.1145/3426972

STEVENS, M. (2008). Foreign Influences on the Japanese Automobile Industry: The Nissan-Renault Mutual Learning Alliance. Asia Pacific Business Review, 14(1), 13–27. https://doi.org/10.1080/13602380701660947

Su, X., Ye, Z., Wu, L., & Shang, Y. (2020). Optimal Stochastic Media Storage in Federated Cloud Environments. 2020 International

Conference on Computing, Networking and Communications, ICNC 2020. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85083442032&doi=10.1109%2fICNC47757.2020.9049482&partnerID=40&md5=9534e77ef35fa68272d870e581761fca

Sullivan, C. (2014). Protecting digital identity in the cloud: Regulating cross border data disclosure. Computer Law & Security Review, 30(2), 137–152. https://doi.org/10.1016/j.clsr.2014.01.004

Sun, G., Liao, D., Anand, V., Zhao, D., & Yu, H. (2016). A new technique for efficient live migration of multiple virtual machines. Future Generation Computer Systems, 55, 74–86. https://doi.org/10.1016/j.future.2015.09.005

Suzic, B., & Reiter, A. (2016). 7. Towards secure collaboration in federated cloud environments. *Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016*. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85015290022&doi=10.1109%2fARES.2016.46&partnerID=40&md5=ba9318ce8a932ce380b22751fd8e2107

T, N. (2020, December 10). What is Federated Cloud? Architecture, Types , Properties & Advantages. *Binary Terms*.

https://binaryterms.com/federated-cloud.html

Terry, S. F. (2014). The Global Alliance for Genomics & Health. Genetic Testing and Molecular Biomarkers, 18(6), 375–376. https://doi.org/10.1089/gtmb.2014.1555

Thakur, P., & Shrivastava, D. K. (2015). Interoperability Issues and Standard Architecture for Service Delivery in Federated Cloud: A Review. 2015 International Conference on Computational Intelligence and Communication Networks (CICN), 908–912. https://doi.org/10.1109/CICN.2015.179

The World Bank. (n.d.). Worldwide Governance Indicators. https://databank.worldbank.org/Institutional-Quality/id/98e680fc

Thomas, M. V., & Chandrasekaran, K. (2017). 34. Dynamic partner selection in Cloud Federation for ensuring the quality of service for cloud consumers. *International Journal of Modeling, Simulation, and Scientific Computing*. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85029718154&doi=10.1142%2fS1793962317500362&partnerID=40&md5=8fdd9141e4eda56ecd703bf37befebb3

Tissir, N., El Kafhali, S., & Aboutabit, N. (2021). Cybersecurity management in cloud computing: Semantic literature review and

conceptual framework proposal. Journal of Reliable Intelligent Environments, 7(2), 69–84. https://doi.org/10.1007/s40860-020-00115-0

Toosi, A. N., Calheiros, R. N., & Buyya, R. (2014). Interconnected cloud computing environments: Challenges, taxonomy, and survey. *ACM Computing Surveys*, *47*(1). https://doi.org/10.1145/2593512

Toosi, A. N., Calheiros, R. N., Thulasiram, R. K., & Buyya, R. (2011). Resource Provisioning Policies to Increase IaaS Provider's Profit in a Federated Cloud Environment. *2011 IEEE International Conference on High Performance Computing and Communications*, 279–287. https://doi.org/10.1109/HPCC.2011.44

Tricomi, G., Merlino, G., Panarello, A., & Puliafito, A. (2020). Optimal selection techniques for Cloud service providers. *IEEE Access*.

U.S. Data Federation. (n.d.). Retrieved June 2, 2023, from https://federation.data.gov/

Vadla, P. K., Kolla, B. P., & Perumal, T. (2020a). 28. FLA-SLA Aware Cloud Collation Formation Using Fuzzy Preference Relationship Multi-Decision Approach for Federated Cloud. *Pertanika Journal of Science & Technology*, *28*(1).

Vaillancourt, P. Z., Wineholt, B., Shepherd, T. J., Pryor, S. C., Lantz, J., Knepper, R., Wolski, R., Myers, C. R., Trumbore, B., Reynolds, R., Sprouse, J., & Lifka, D. (2021). Aristotle Cloud Federation: Container Runtimes Technical Report (arXiv:2109.12186). arXiv. https://doi.org/10.48550/arXiv.2109.12186

Value and alliance capability and the formation of strategic alliances in SMEs: The impact of customer orientation and resource optimisation—ScienceDirect. (n.d.). Retrieved May 31, 2023, from https://www.sciencedirect.com/science/article/pii/S014829631830095X?via%3Dihub

Veloso, B., Malheiro, B., & Carlos Burguillo, J. (2016). CloudAnchor: Agent-Based Brokerage of Federated Cloud Resources. In Y. Demazeau, T. Ito, J. Bajo, & M. Escalona (Eds.), ADVANCES IN PRACTICAL APPLICATIONS OF SCALABLE MULTI-AGENT SYSTEMS: THE PAAMS COLLECTION (Vol. 9662, pp. 207–218). IEEE Syst Man Cybernet Soc Spain; IBM; AEPIA; AFIA; APPIA; Polytechn Univ Madrid; Univ Seville; CNRS; Ingn Software Avanzado S A; Indra; Portuguese Assoc Artificial Intelligence; Assoc Francaise Intelligence Artificielle; IEEE Secc Espana; Fundac Investigac Desarrollo Tecnologias Informac

Andalucia; Escuela Tecnica Super Ingn Informatica. https://doi.org/10.1007/978-3-319-39324-7_18

Vincenzo, S., & Jan. (2020). *International agreements on cross-border data flows and international trade: A statistical analysis* (OECD Science, Technology and Industry Working Papers No. 2020/09; OECD Science, Technology and Industry Working Papers, Vol. 2020/09). https://doi.org/10.1787/b9be6cbf-en

Voigt, P., & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide (1st ed. 2017). Springer International Publishing : Imprint: Springer. https://doi.org/10.1007/978-3-319-57959-7

Wahab, O. A., Bentahar, J., Otrok, H., & Mourad, A. (2018a). Towards Trustworthy Multi-Cloud Services Communities: A Trust-Based Hedonic Coalitional Game. *IEEE Transactions on Services Computing*. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85042018726&doi=10.1109%2fTSC.2016.2549019&partnerID=40&md5=2f0a7adf7ffba904d17fea0ab18b3a68

Wang, F.-K., & He, W. (2014). Service strategies of small cloud service providers: A case study of a small cloud service provider and its clients in Taiwan. *International Journal of Information*

Management, *34*(3), 406–415. https://doi.org/10.1016/j.ijinfomgt.2014.01.007

Wang, X., Wang, X., Che, H., Li, K., Huang, M., & Gao, C. (2015). An Intelligent Economic Approach for Dynamic Resource Allocation in Cloud Services. *IEEE Transactions on Cloud Computing*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84940984822&doi=10.1109%2fTCC.2015.2415776&partnerID=40&md5=e083b472f75b03e397be7fabe33214bc

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, *26*(2), xiii–xxiii.

What is enterprise federation and how does it work with VMware Cloud Services. (2022, November 3). https://docs.vmware.com/en/VMware-Cloud-services/services/Using-VMware-Cloud-Services/GUID-358D70A6-DB33-4673-B2D6-43C73A1051FD.html

Wu, S., Wu, Z., Wu, X., Tao, J., & Gu, Y. (2022). 15. Queuing-Based Federation and Optimization for Cloud Resource Sharing. *Information (Switzerland)*. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85136791386&doi=10.3390%2finfo13080361&partnerID=40&m

d5=2bdf5110ec7168a4dc9f1e4bf2a4bf75

Xu, J., & Palanisamy, B. (2021). 19. Optimized Contract-Based Model for Resource Allocation in Federated Geo-Distributed Clouds. *IEEE Transactions on Services Computing*. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85040994787&doi=10.1109%2fTSC.2018.2797910&partnerID=40&md5=ced229d0d5c9e0a1fb18bba20eabb3bc

Xu, Z.-W., Li, Z.-Y., Yu, Z.-S., & Li, F.-Z. (2023). Information Superbahn: Towards a Planet-Scale, Low-Entropy and High-Goodput Computing Utility. *Journal of Computer Science and Technology*, *38*(1), 103–114. https://doi.org/10.1007/s11390-022-2898-7

Yasuda, H. (2005). Strategic alliances for SMEs. https://www.semanticscholar.org/paper/Strategic-alliances-for-SMEs-Yasuda/ea04ba13d326673fa156f92f580b32cf5d1c8a6c

Yu, J., Malerba, F., Adams, P., & Zhang, Y. (2017). Related yet diverging sectoral systems: Telecommunications equipment and semiconductors in China. Industry and Innovation, 24(2), 190–212. https://doi.org/10.1080/13662716.2016.1224709

Zamir, Z., Sahar, A., & Zafar, F. (2014). *Strategic Alliances ; A*

Comparative Analysis of Successful Alliances in Large and Medium Scale Enterprises around the World. https://www.semanticscholar.org/paper/Strategic-Alliances-%3B-A-Comparative-Analysis-of-in-Zamir-Sahar/1c7273d5be2dc4573f44ea8327ddeed1a5471aaa

Zant, B. E., Zant, N. E., Kadhi, N. E., & Gagnaire, M. (2013). Security of Cloud Federation. *2013 International Conference on Cloud Computing and Big Data*, 335–339. https://doi.org/10.1109/CLOUDCOM-ASIA.2013.93

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications*, *1*(1), 7–18. https://doi.org/10.1007/s13174-010-0007-6

Appendix 1

Table 7: Summary of the studies (N/A stands for 'Not Applicable')

Paper ID	Reference	Title of the Study	Purpose of the study	Current Trends					
				Cloud federation formation Theories	**Parameters (Factors) Influencing cloud federation formation**	**Proposed Solution (Methodology)**	**Evaluation parameter** *(Ref Figure 13)*	**Experiment Approach**	**Experimentation Tools**
P1	Chen,et.al. (2017)	"Workload Factoring and Resource Sharing via Joint Vertical and Horizontal Cloud Federation Networks"	"The study aims to establish Horizontal and Vertical (Joint) cloud federation for comprehensive and efficient cloud collaboration."	Hedonic Coalition Game Theory	Utility, other	Algorithm & model	O3, O1,C1, C7, P4, U1, C8, PT1	Simulation Analysis	Java
P2	Fan, et.al (2018)	"VM instance selection for deadline constraint job on agent-based interconnected cloud"	"To enhance the efficiency of users managing VM instances, this research introduces the concept of Instance Group (IG)."	Set Theory (Rough Set Model)	Resource Information	Algorithm & model	A1, QoS6, PT2	Simulation Analysis	Hadoop MapReduce Application
P3	Udhayakumar, et.al. (2019)	"Trustworthy Cloud Federation Through Cooperative Game Using QoS Assessment"	"The study aims to design an efficient mechanism for identifying trustworthy cloud service providers in the Heterogeneous cloud environment."	Cooperative Game theory	Trust SLA (QoS) Parameters	Model	U6, R4	Real-time Cloud Environment testbed	OpenStack
P4	Gupta, et.al. (2016)	"Trusted partner selection in broker based cloud federation"	"Creating a cloud federation through the utilization of trust factors to categorize foreign clouds based on their past performance and	Other	Trust	Algorithm & model	P2, R1, R2	Simulation Analysis	CloudSim

			recommendations from neighboring entities."						
P5	Wahab, et.al. (2018)	"Towards Trustworthy Multi-Cloud Services Communities: A Trust-Based Hedonic Coalitional Game"	"Developing trust-based hedonic coalitional games to facilitate the decentralized formation of dependable multi-cloud communities"	Hedonic Coalition Game Theory with (Non-Transferable utility)	Trust Resource Information	Algorithm & model Framework	R3, QoS2, PT1, PT3, P1, A2	Simulation Analysis	Matlab
P6	Halabi & Bellaiche (2020)	"Towards Security-Based Formation of Cloud Federations: A Game Theoretical Approach"	"Creating measurable Cloud Security-SLA parameters, assessing the security standards of CSP and federations, and constructing a game-theoretic model for the formation of security-focused Cloud federations."	Hedonic Coalition Game Theory	SLA Parameters, Security	Algorithm & model	QoS3, QoS4, QoS5, P1, PT1	Simulation Analysis	MATLAB
P7	Suzic & Reiter (2016)	"Towards secure collaboration in federated cloud environments"	"The aim is to propose a novel Zoned security model for federated cloud environments, organizing them into zones with equivalent data security requirements."	N/A	Security	Use Case-Analysis	N/A	N/A	NA
P8	Ray, et.al(2019)	"Toward maximization of profit and quality of cloud federation: solution to cloud federation formation problem"	"The goal is to establish a cloud federation that optimizes federation profit while simultaneously achieving a balance between the QoS and the profit of individual cloud federation members."	(Linear Programming Method) Integer Linear Program with Heuristic Algorithm	Utility, SLA (QoS) Parameter	Framework, Model & Algorithm	U1, U2, QoS1, PT1	Simulation Analysis	Python (Lpsolve Python API)

P9	Falasi, & Serhani, (2017)	"SLA Specification and Negotiation Model for a Network of Federated Clouds: CloudLend"	"The objective is to put forth a weighted SLA specification model for effective management of SLA requirements, along with a game theory-based automated SLA negotiation model that encompasses QoS monitoring capabilities."	Game Theory	SLA (QoS) Parameter	Algorithm & model	A3, A4	Simulation Analysis	CloudLend
P10	Massonet, et.al(2016)	"Security requirements in a federated cloud networking architecture"	"Offer the security architecture for the BEACON project."	N/A	Security	Architecture and Analysis	N/A	N/A	NA
P11	Kirthica, & Sridhar, et.al. (2018)	"Securely communicating with an optimal cloud for intelligently enhancing a cloud's elasticity"	"Enhancing cloud elasticity securely by interacting with an external cloud for additional resources when needed."	Kerberos Protocol	Security SLA (QoS) Parameter	Algorithm & model	PT5, PT6	Real-time Cloud Environment testbed	Eucalyptus, OpenStack, OpenNebula
P12	Bouabdallah, et.al. (2017)	"Resources provisioning within cloud federation"	"Creating a horizontal cloud federation for collaborative business opportunities, including energy saving, on-demand resources, and cost optimization."	Contract Net Protocol	SLA (QoS) Parameter Resource information, Open Virtualization Format standard	Protocol & Standard	P5, QoS9	Real-time Cloud Environment testbed	Testbed (Open Nebula, JADE platform
P13	Alam, et.al (2020)	"Reliability-based Formation of Cloud Federations Using Game Theory"	"Through bolstering cloud providers' reliability, forming cloud federations, and preventing cooperation with untrustworthy CSPs."	Hedonic Coalition Game Theory	SLA (QoS) Parameter, Trust	Algorithm & model	R5, QoS4, PT5	Simulation Analysis	MATLAB CloudSim
P14	Mourougan,& Aramudhan, (2016)	"Regression tree based ranking model in federated cloud"	"Proposing an effective trust-based methodology using SMI attributes and regression tree model to enhance security and privacy in the federated cloud."	Regression Tree Model	Trust (past behavior of CSP) SLA (QoS) Parameter, Cost	Model	PT1, PT3	Simulation Analysis	Cloud Sim (JADE platform)

P15	Wu, et.al (2022)	"Queuing-Based Federation and Optimization for Cloud Resource Sharing"	"Proposing CLFS, a Pareto optimal resource sharing solution, enabling individual cloud autonomy in strategy selection and simplified service request allocation and profit sharing for federation formation."	N/A	Cost Utility of providers	Algorithm & model	QoS7, U4	Simulation Analysis	Not Specified
P16	Ray, et.al(2021)	"Quality and Profit Assured Trusted Cloud Federation Formation: Game Theory Based Approach"	"Introducing a broker-based cloud federation architecture that aims to maximize overall profit and availability within a federation formed among trusted CSPs".	Hedonic Coalition Game Theory	Trust Utility (Satisfaction of the QoS(availability) and profit)	Algorithm & model(cost model)	U1, U2, U3, U4, QoS2, QoS1,P1, PT1	Simulation Analysis	Python (to estimate the parameter of beta mixture models, statistical software Used)
P17	Ahmed, et,al (2021)	"QoS-aware trust establishment for cloud federation"	"Proposing a method that employs a QoS-aware trust evaluation mechanism, enabling the assessment of participating CSPs based on a shared feature space."	N/A	Trust SLA (QoS) Parameters Resource Information	Architecture & Model	QoS1,PT2	Real-time Cloud Environment testbed	Pythons (for Agent development) CometCloud and C4C Federate cloud system
P18	Hassan, et.al.(2016)	"QoS and trust-aware coalition formation game in data-intensive cloud federations"	"Solving efficient cloud provider federation through AI for dynamic user resource needs in data-intensive workloads."	Hedonic Coalition Game Theory	SLA (QoS) Parameters Trust	Algorithm & model (Mathematica model)	P4, U2, U1, C2, C3	Simulation Analysis	Other
P19	Xu, & Palanisamy, (2021)	"Optimized Contract-Based Model for Resource Allocation in Federated Geo-Distributed Clouds"	"Introducing a new contracts-based resource sharing model for federated geo-distributed clouds, allowing CSPs to establish agreements with data centers for defined time intervals in a 24-hour period."	Game Theory (Heuristic techniques for Auction mechanism)	Cost Other (Job Schedule)	Algorithm & model	C2, PT5, P4, P6, U2	Simulation Analysis	Other simulator SHARCNET cluster trace

P20	Abusitta, et.al. (2018)	"On trustworthy federated clouds: A coalitional game approach"	"Developing a decentralized framework for cloud federation formation based on Objective and Subjective trust evaluation of heterogeneous CPs."	Hedonic Coalition Game Theory	Trust	Algorithm & model	QoS2, PT1, PT3, R3, R4	Simulation Analysis	CloudSim
P21	Hammoud, et.al (2018)	"On the detection of passive malicious providers in cloud federations"	"Designing a maximin game theoretical model to detect passive malicious providers and maximize overall monetary profit for cloud broker and providers through federation, while enhancing customer QoS."	Maximin Game Theory model	Resource information Trust	Model	R3, U1, PT4, QoS2	Simulation Analysis	MATLAB CloudHarmony Dataset
P22	Moghaddam, et.al(2020)	"On Coordination of Smart Grid and Cooperative Cloud Providers"	"Creating a synergy between a smart grid and autonomous cloud providers operating collaboratively as cloud federations, within the framework of a dynamic electricity pricing scheme."	Stackelberg game	Cost Utility (Individual Profit) Resource Information(User workload)	Model	U1, U2	Simulation Analysis	MaTLAB YALMIP toolbox
P23	Romero & Altmann, (2017)	"Model for incentivizing cloud service federation"	"Analyzing the drivers that promote business collaboration and strategic alliances within the cloud computing industry sector."	Game Theory	Utility of the providers	Model (mathematical)	P3, U6, U1, U3	Simulation Analysis	Agent Based modeling tools
P24	Ray, et.al (2018)	"Migration cost and profit-oriented cloud federation formation: hedonic coalition game based approach"	"Creating a cloud federation with the goal of maximizing profit while minimizing migration costs."	Hedonic Coalition Game Theory	Profit Migration cost	Algorithm & model	U3, C4, U1, U2, P1, QoS1	Simulation Analysis	CloudHarmony Dataset
P25	Farris, et.al (2017)	"MIFaaS: A Mobile-IoT-Federation-as-a-Service Model for dynamic cooperation of IoT Cloud Providers"	"Introducing MIFaaS, a novel paradigm enabling dynamic cooperation between private and public clouds of IoT devices."	Game Theory	Utility of the providers SLA (QoS) Parameters Resource Information	Algorithm & model	C1, U4, QoS8, P1, P3, PT2	Simulation Analysis	Matlab

P26	Javed, et.al(2020)	"IoTEF: A Federated Edge-Cloud Architecture for Fault-Tolerant IoT Applications"	"Proposing the IoTEF architecture for multi-cluster IoT applications, focusing on fault tolerance, and formulating functional and non-functional requirements."	N/A	N/A	Framework	PT4, PT3, QoS11, QoS8	Real-time Cloud Environment testbed	Testbed (Raspberry Pi 2 Model B+, Ubuntu VM, Linux Server)
P27	Moreno-Vozmediano, et.al(2017)	"Implementation and Provisioning of Federated Networks in Hybrid Clouds"	"The paper proposes a cloud network federation framework integrated with OpenNebula, facilitating automatic provisioning of cross-site virtual networks for interconnecting geographically distributed cloud infrastructures."	N/A	N/A	Framework	QoS11, PT3	Real-time Cloud Environment testbed	OpenNebula and Amazon EC2
P28	Vadla,et.al(2020)	"FLA-SLA Aware Cloud Collation Formation Using Fuzzy Preference Relationship Multi-Decision Approach for Federated Cloud."	"Proposing an FLA-SLA-based cloud federation formation strategy that selects a collated provider list for maximizing profit from available resources."	Hedonic Coalition Game Theory	SLA (QoS) Parameters	Algorithm & model	PT1, U1, P1	Simulation Analysis	Matlab
P29	Gonzalez-Compean, et.al(2018)	"FedIDS: a federated cloud storage architecture and satellite image delivery service for building dependable geospatial platforms"	"The paper showcases the creation of a Federated Cloud Storage Architecture (Fed) and Satellite Image Delivery Service (IDS) for building reliable geospatial platforms."	N/A	N/A	Architecture	QoS10, PT3, QoS8	Real-time Cloud Environment testbed	Real time implementation
P30	Celesti, et.al(2016)	"Federated Networking Services in Multiple OpenStack Clouds"	"The paper outlines initial findings of a novel Federation management system design, aiming to offer federated networking services across multiple OpenStack clouds within a federation."	N/A	Security	Architecture	N/A	Real-time Cloud Environment testbed	OpenStack

P31	Khandelwal, et.al(2016)	"Fast algorithms for optimal coalition formation in federated clouds"	"Proposing a fast polynomial time greedy algorithm for optimal federation formation and equitable payoff distribution using exact Banzhaf indices for individual cloud service providers."	Hedonic Coalition Game Theory	Utility (Profit) Resource Information	Algorithm & model	PT1, U2	Simulation Analysis	Other
P32	Verghelet, et.al(2017)	"Efficient P2P Inspired Policy to Distribute Resource Information in Large Distributed Systems"	"Proposed a pBN-based resource information policy that helps to select the efficient node to communicate."	Grid Matrix	Resource Information Trust (feedback from a neighbor)	Policy (Best Neighbor Policy)	Emergent cloud federation Modularity, Scalability, P1,	Simulation Analysis	SimGrid
P33	Darzanos, et.al (2016)	"Economics models and policies for cloud federations"	"The authors propose a model for cloud federations, featuring three modes—strong, weak, and elastic—with different levels of CSP interaction in workload forwarding."	Non-cooperative game	SLA (QoS) Parameters Energy Consumption cost Utility(Individual CSPs Revenue)	Model & Policies	U1, U2, P6, QoS1	Simulation Analysis	Other
P34	Thomas & Chandrasekaran, (2017)	"Dynamic partner selection in Cloud Federation for ensuring the quality of service for cloud consumers"	"The paper proposes an AHP and TOPSIS-based partner selection mechanism for the Cloud Federation, considering trust values of individual CSPs."	Set Theory (AHP and TOPSIS method)	SLA (QoS) Parameters Trust	Algorithm & model	P2, R2, QoS1	Simulation Analysis	CloudSim
P35	Shrivastava & Pateriya (2020)	"Data encoding and cost optimized distribution for efficient and secure storage in cloud federation"	"Develops an easy-to-use method for storing, retrieving, and managing identities for Cloud Federation that drives adoption."	Linear Programming Method	SLA (QoS) Parameters	Algorithm/ Framework & model	C5, PT1	Simulation Analysis	CloudSim

P36	Li, et.al (2021)	"Cooperative Service Placement and Scheduling in Edge Clouds: A Deadline-Driven Approach"	"Introduces an innovative online framework for joint cooperative placement and scheduling, leveraging spatial-temporal diversities in workload and resource costs across federated edge clouds (Ecs)"	auction-Based Mechanism	Resource Information	Algorithm & model	C1, PT2, U4	Simulation Analysis	Other
P37	Ayachi, et.al (2021)	"Cooperative game approach to form overlapping cloud federation based on inter-cloud architecture"	"Puts forward three cloud federation formation protocols grounded in cooperative game theory and develops unique mechanisms designed to create federations that maximize the total profit."	Non-Transferable Utility Game Theory (Partition function and Overlapping Coalition game)	SLA (QoS) Parameters Costs	Comparative Study/ Algorithm/ Mathematical Models	U1, P1, PT1	Simulation Analysis	* Cloud sim (LpSolve library, and JasperReport tool)
P38	Biran & Dubow (2019)	"Confederated cloud—Design consideration for distributed utility computing system of systems"	"Proposes an interim solution for decentralized SoS with grouped multi-CSP deployments."	N/A	SLA (QoS) Parameters	Design & Mathematical model	C1, QoS1, Load Balancing	Conceptual Analysis	NS
P39	Comi & Fotia (2018)	"Combining reliability, reputation and honesty to enhance QoS on federated computing infrastructures"	"Introduces an agent-based model for optimizing QoS in a computing infrastructure federation and proposes the Friendship and Group Formation (FGF) algorithm to maximize global utility."	Agent-Based Model	Trust (based on reliability and reputation (feedback based)) SLA (QoS) Parameters	Algorithm & model	P4, O2	Simulation Analysis	Agent Based Modeling tool
P40	Satheesh & Aramudhan (2019)	"Cloud ranking model for optimal service selection based on random fuzzy logic"	"Discuss different ranking methods and propose one based on random variable selection in ranking."	Set Theory (Fuzzy Preferential Ranking system)	SLA (QoS) Parameters Resource Information Cost	Algorithm & model	PT1, PT2	Simulation Analysis	JAVA

P41	Darzanos, et.al (2019)	"Cloud federations: Economics, games and benefits"	"The goal is to develop a core theory for the sharing economy of computing resources among CSPs, presenting novel federation models and policies for profitable collaborations with satisfactory QoS."	Non-cooperative game	SLA (QoS) Parameters Utility (Profit)	Economic Policy	Restriction on Best possible QoS and Customers willingness to pay QoS9, U1, U2, QoS1, PT4, R3, C6,	Simulation Analysis	other
P42	Hammoud, et.al (2020)	"Cloud federation formation using genetic and evolutionary game theoretical models"	"The purpose of this paper is to improve profit while maintaining federation stability, and to achieve optimal profit and federation stability."	Game Theory(heuristic genetic algorithm (GA) & Evolutionary game)	SLA (QoS) Parameters Cost	Algorithm & model	U1, U3, QoS1, QoS8	Simulation Analysis	Matlab CloudHarmony
P43	Khandelwal, et.al(2018)	"Cloud Federation Formation in Oligopolistic Markets"	"The authors employ cooperative game theory to investigate whether peer-to-peer federation or using a broker is more advantageous for cloud providers."	Cooperative Game theory (Linear Production Game)	Cost	Model	P1, U2, PT1	Simulation Analysis	Other
P44	Psomakelis, et.al.(2018)	"BUDaMaF data management in cloud federations"	"Presents a BUDaMaF which is a novel multi-cloud federation data management framework that was developed in the context of a collaborative Korean-European project called BASMATI to meet its data management needs."	N/A	N/A	Architecture and framework	N/A	Case Analysis	Other
P45	Zefferer, et.al (2018)	"Best of two worlds: Secure cloud federations meet eIDAS"	"Provides a method for restricting data access to authorized users who have been granted the necessary privileges."	N/A	Security	Other	N/A	Real-time Cloud Environment testbed	SUNFISH Infrastructure

P46	Najm and Tamarapalli (2022)	"Towards cost-aware VM migration to maximize the profit in federated clouds"	"Develop a VM and migration cost model within a federated cloud to tackle the challenge of inter-DC VM migration, aiming to minimize the overall operational cost."	N/A	N/A	Framework	N/A	Simulation Analysis	CloudSim
P47	Zeng et al., (2022)	"Game strategies among multiple cloud computing platforms for non-cooperative competing assignment user tasks"	"Strategy to analyze competition and cooperation among CSPs and establish a collaborative cloud federation."	N/A	NS	Framework	N/A	Simulation Analysis and Case Analysis	Matlab
P48	Hadjres, et.al(2021)	"An SLA-aware cloud coalition formation approach for virtualized networks"	"Introduces a novel social gaming-based approach for cloud coalition formation, aiming to identify the optimal coalition of cloud providers that can effectively respond to requests while satisfying clients' SLA requirements."	Hedonic Coalition Game Theory with (Transferable Utility game)	Resource Information SLA (QoS) Parameter Cost	Algorithm & model (Mathematical)	PT1, U1, U2, P1, P4	Simulation Analysis	Matlab
P49	Li et al.,(2022)	"Agent-based multi-tier SLA negotiation for intercloud"	"Proposed AFCN model for fully distributed and autonomous intercloud approach."	N/A	NS	Framework and extended Protocol	Query Time PT1, PT2	Simulation Analysis	Cloudsim
P50	Dhole, et.al. (2016)	"An efficient trust-based Game-Theoretic approach for cloud federation formation"	"The study proposes a game-theoretic model to form cloud federations, taking the trust of CSPs into account during the formation process, and maximizing the CF profit."	Cooperative Game theory	Trust Resource Information and cost Individual utility	Algorithm & model	R2, U1	Simulation Analysis	CloudSim
P51	Maria & Aramudhan, (2017)	"An efficient technique for trust based cloud providers ranking in federated cloud"	"The strategy involves measuring CSP trust and ranking them using fuzzy score values. By considering various trust factors and applying fuzzy logic,	Set Theory (Fuzzy Logic based Classification and Superior ABC algorithm)	Security Trust	Algorithm & model	PT1, P2, PT2, QoS8	Simulation Analysis	CloudSim

			the CSPs are evaluated and ranked based on their trustworthiness."						
P52	Bouchareb & Zarour (2021)	"An agent-based mechanism to form cloud federations and manage their requirements changes"	"Introduce an agent-based mechanism to autonomously manage Cloud federations and adapt to changing requirements, accepting additional requests with minimal cost and energy consumption, while actively selecting the best Cloud providers."	Offer Strategy and Acceptance Strategy	SLA (QoS) Parameter Cost(Price of the resource, Energy consumption)	Case study & Model	U1	Simulation Analysis Case Study Analysis	Agent Based Modeling Tool
P53	Mashayekhy, et.al(2021)	"A Trust-Aware Mechanism for Cloud Federation Formation"	"Maximizing the CF profit by establishing the CF with highly reputable CSP."	Cooperative Coalitional Game theory with (Transferable Utility game)	Resource Information Trust graph (CSPs Reputation)	Algorithm & model	R2, U2, P1, PT1,	Real-time Cloud Environment testbed	MapReduce, Hadoop Cluster (TeraSort)
P54	Kansal, et.al. (2020)	"A request allocation model for processing data in federated cloud computing"	"Presents framework for resource distribution to improve the revenue using a cooperative game theory."	Hedonic Coalition Game Theory	SLA (QoS) Parameter	Algorithm & model	U2, U6	Simulation Analysis	Matlab
P55	Comi, et.al.(2016)	"A partnership-based approach to improve QoS on federated computing infrastructures"	"Proposed a Friendship and Group Formation algorithm that allows CSPs to select their partners to improve the global QoS."	Set Theory	Resource Information Trust (feedback and Recommendation based)	Algorithm & model	O2, U5	Simulation Analysis	GNU Octave
P56	Nemati, et.al.(2019)	"A novel game theoretic approach for forming coalitions between IMS cloud providers"	"Using a method inspired by the stable roommate matching algorithm, establish a stable coalition of IMS cloud infrastructure providers."	Game Theory (Stable roommate matching algorithm)	Resource Information Cost	Algorithm & model	U1, QoS8, PT1	Simulation Analysis	Matlab

P57	Latif, et.al. (2021)	"A novel cloud management framework for trust establishment and evaluation in a federated cloud environment"	"It presents an evaluation framework for trust that identifies issues of trust establishment between CSPs, evaluates levels of trust, and establishes a cloud federation with a trusted CSP."	N/A	Trust (feedback based and SLA based) SLA (QoS) Parameter	Model Framework	R2	Real-time Cloud Environment testbed	Java J2EE Eclipse development platform MYSQL OpenStack
P58	Hadjres, et.al(2021)	"A green, energy, and trust-aware multi-objective cloud coalition formation approach"	"Providing a practical, scalable, and adaptable SLA-based approach to cloud federation formation."	multi-objective Hedonic Coalition Game Theory (roommate matching algorithm)	Resource Information Cost (resource, mislocalization, mis-truthfulness) Other (Green tag of each server)	Algorithm & model	U1, P1, U2, C2, C3, C6, PT1	Simulation Analysis	MATLAB
P59	Neda, et.al.(2020)	"Resource management in the federated cloud environment using Cournot and Bertrand competitions"	"To solve heterogeneous resource management problems and increase collaboration between cloud providers, this study proposes a new resource management model based on Cournot and Bertrand games."	"Game Theory (Cournot and Bertrand games)"	Resource information Number of resource Price	Model	U1	Simulation Analysis	CloudSim
P60	Dinachali, et.al. (2022)	"A cost-aware approach for cloud federation formation"	"Establish an optimal cloud federation that maximizes profit for service providers in order to keep them in the federation."	"Cooperative Game theory (Greedy Algorithm)"	Resource Information expected profit (Utility), Cost	Algorithm & model	U6, P2, P4, P2, R2, U1	Real-time Cloud Environment testbed	Not Specified
P61	Halabi, et.al.(2018)	"A cooperative game for online cloud federation formation based on security risk assessment"	"Provide a security risk assessment approach and evaluate the security risk levels of CSPs then establish a Cloud federation based on a hedonic coalitional game."	Hedonic Coalition Game Theory	Security Trust(security reputation) SLA (QoS) Parameter	Algorithm & model	PT1	Simulation Analysis	MATLAB

P62	Pacini, et.al. (2019)	"A Bio-inspired Datacenter Selection Scheduler for Federated Clouds and Its Application to Frost Prediction"	"Demonstrate a multiobjective broker policy that selects data centers based on network latency, monetary cost, and resources availability to ensure efficient and reliable execution of FPA-jobs across geographically distributed datacenters."	Ant Colony Optimization (ACO) and Particle Swarm Optimization (PSO),	Resource Information	Algorithm & model	QoS9	Simulation Analysis	CloudSim
P63	Shi, et.al. (2022)	"A Bayesian game-enhanced auction model for federated cloud services using blockchain"	"The study proposes a federated auction model using Bayesian game theory and blockchain to model ineffective information sharing among auction participants and to enhance the effectiveness and trustworthiness of the cloud auction."	Bayesian Game Theory	SLA (QoS) Parameter Cost	Algorithm & model	Auction commission fee QoS10, U6, PT1, C1, C2, C3,	Simulation Analysis	NS

Acknowledgments

This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the Human Resource Development Project for Global R&DB Program (IITP-2019-0-01328) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation).

Abstract (Korean)

클라우드 컴퓨팅은, 소비자들에게 신기술에 대한 접근, 혁신성 및 확장성 등 다양한 혜택을 제공하며 빠르게 성장하고 있다. 그러나 클라우드 컴퓨팅 시장은 주로 대기업의 영향력이 지배적이어서, 중소규모의 클라우드 공급자들의 시장 경쟁력이 제한되고 있다. 중소규모 클라우드 공급자들의 경쟁력 향상을 위해, 서로 다른 목적을 가진 여러 클라우드 공급자를 활용하는 멀티 클라우드 전략(multi-cloud strategy)을 채택할 수 있다. 이러한 멀티 클라우드 전략을 구현하는 한가지 방법에는 클라우드 연합(cloud federation)이 있는데, 클라우드 연합은 클라우드 공급자가 필요에 따라 다른 공급자의 서비스를 사고 팔 수 있게 하는 것으로, 클라우드 서비스의 안정성을 높이고, 비용과 에너지 소비를 줄이며, 리소스를 쉽게 확장하는 장점을 가지고 있다.

본 논문은, 클라우드 연합 형성에 대한 설득력 있고 포괄적인 조사를 수행하는데 그 목적이 있으며, 이를 위해 두가지 주요 연구가 수행되었다. 첫번째 연구는, 클라우드 연합 형성에 대한 기여 요인, 요구사항, 도전 과제, 현재 동향과 관련한 체계적인 문헌 고찰(systematic literature review)을 진행하였다. 그리고 문헌 고찰을 토대로, 혁신적인 기관 품질 인식 신뢰 클라우드 연합 형성 (Institutional Quality-Aware Trusted Cloud Federation Formation) 방법을 제안하였으며, 이를 통해 클라우드 연합 형성의 복잡성과 불확실성을 해결할 수 있도록 하였다. 또한, 제안된 방법으로, 새로운 클라우드 연합의 전체 아키텍처와 연합 형성 알고리즘을 도입하고, 클라우드 서비스

공급자가 신뢰할 수 있는 파트너를 선택할 수 있도록 2 단계 신뢰 평가 프로세스를 제안하였다.

본 연구에서는, 클라우드 연합 형성을 포괄적으로 조사하기 위해 6 개의 연구 질문을 설정하였다. 첫번째 연구인 체계적 문헌 검토(systematic literature review)를 통해서는 6 개 연구 질문 중 4 개의 연구 질문을 다루었으며, 16 가지 클라우드 연합 구성 활성화 요인, 17 가지 요구 사항, 18 가지 주요 과제를 성공적으로 확인하였다. 활성화 요인 중에서 리소스 프로비저닝(provisioning)과 유연성이 가장 많이 논의되는 요인이었으며, 법률 문제와 규정 준수는 상대적으로 덜 논의되고 있었다. 요구사항과 관련해서는, 클라우드 서비스 공급자 간의 신뢰와 평판이 가장 광범위하게 연구되었으며, 신뢰와 평판은 성공적인 클라우드 연합 구성에 중요한 요소로 강조하였다. 또한, 클라우드 연합의 안정성은, 문헌 검토에서 클라우드 연합 구성을 위한 중요한 과제로 드러났으며, 가장 많이 사용된 연구 동향은, 게임이론(game theory)과 집합이론(set theory)으로, 주로 알고리즘적 접근과 수학적 모델을 중심의 해결책이 제안되었다.

두번째 연구에서는, 6 개 연구 질문 중 2 개를 다루기 위해 기관 품질 인식 신뢰 클라우드 연합 형성 접근법(institutional quality-aware trusted cloud federation formation approaches)을 제시하였다. 이 혁신적인 접근법은 2 단계 신뢰 평가 과정(two-stage trust evaluation process)을 활용하는데, 첫번째 단계에서는 CSP 신뢰와 기관 신뢰를 계산하여, CSP 전체 신뢰를 결정하였다. 이어서 두번째 단계에서는 CSP 와 사용자로부터의 직접적, 간접적 피드백을 통해 신뢰를 집계하였다.

피드백 집계에 신뢰도 점수를 포함시킴으로써, 이 접근 방법은 거짓 긍정과 거짓 부정의 위험을 효과적으로 줄일 수 있었다. 제안된 모델은 두가지 실험을 통해 평가되어, 신뢰할 수 있는 연합 파트너를 확인하는데 효과적임을 입증하였다. 이러한 연구 결과는, 클라우드 연합 형성에 있어, 신뢰 인식 접근법의 중요성을 강조하고, 멀티 클라우드 전략(multi-cloud strategy)의 신뢰성과 성공확률을 높이는데 가치 있는 통찰력을 제시하였다. 나아가, 본 연구는 클라우드 서비스 공급자 간의 협업 촉진에 기여할 수 있으며, 중소규모 클라우드 서비스 공급자가 클라우드 컴퓨팅 시장의 지배적인 공급자와 효과적으로 경쟁할 수 있도록 기회를 제공하였다.

주요어: 신뢰할 수 있는 클라우드 연합, 기관 품질, 신뢰, 규제 품질, 클라우드 연합 형성, 클라우드 협력 형성, 협력 형성

학 번: 2020-32099