Effect of Trust and Institutional Quality on Cloud Federation Formation using Agent-Based Modeling

Yodit Gebrealif[1] [0000-0001-6536-7290], Jörn Altmann[1] [0000-0002-8880-9546]
[1] Technology Management, Economics, and Policy Program,
Seoul National University
South Korea
yodit.gebrealif@gmail.com,jorn.altmann@acm.org

Abstract. Trust between cloud service providers is an important characteristic that helps the provider to make a decision on whom to interact with. However, achieving trust has been a major challenge that hinders cloud federation adoption. Numerous researchers observed trust from the provider's side, but one's trust can also be affected by the environment (e.g., culture, availability of legal framework) and also by policies or strategies monitored by a state. Moreover, the cloud federation model allows various participants from different countries to join and work together including resource sharing, data transferring, and knowledge sharing. Data transport is a sensitive issue and needs a legal framework when data is transferred from one country to another. However, the data protection concern is not met equally in all countries, and it impacts the trust between participants. Therefore, this paper addresses trust with data protection challenges and proposes a trust evaluation mechanism for cloud federation formation in the partner selection stage. The proposed trust evaluation model utilizes neighbors' feedback and institutional trust, to evaluate cloud service provider trust and data protection parameters. The evaluation of the model is conducted by using an agent-based approach and the Netlogo simulation tool. The results show that the proposed model generates more profit than a CSP trust model without institutional trust.

Keywords: Trusted cloud federation, Institutional quality, Trust, Regulatory quality, Cloud federation formation, Cloud coalition formation, Agent-based modeling, Agent-based simulation, Cooperative formation, Institutional quality, Regulatory quality, Rule of law.

1 Introduction

Cloud computing brings a large number of services to customers with low infrastructure costs. Customers access these services, work online, and store their data in the cloud. Data is stored in the cloud without the customers knowing where the data is located and relocated, who is accessing the data, or from where the data is accessed [1]. As a consequence, data privacy, protection, and confidentiality have become the major issue in cloud computing. Especially in the data economy era, data is the future economic power to the government and enterprises. Consequently, the government and cloud service providers (CSP) need to assure that the client's data is protected and safe [2], [3]. The data safety issue is even more challenging when it comes to cloud federation (CF), which allows CSP to rent the resources from another provider when the demand exceeds the supply, and to rent out whenever other providers need to share their loads[4], [5]. During this process, the customer data can be located or relocated to different countries with an agreement between the CSPs but without a cloud customer's consent. It affects the trust between the CSP and cloud customers [3].

Figure 1: Logical representation of CSPs integration

Trust establishment and evaluation across CSPs have been defined as a prerequisite and critical requirement for participation in a CF, to utilize computing resources effectively [5], [6]. Trust in cloud federation refers to the home cloud perception regarding the foreign cloud behaviors, which influences the decision of the home cloud to choose the foreign cloud and establish a CF [4], [7], [8]. It is a factor that has long been seen as a measure of evaluation, which serves as a foundation for decision-making regarding the extent to which the entity would behave as predicted. This measure of assessment needs some input to be calculated. In this research, those inputs are called factors (determinants) and are explored. Apart from these determinants, trust has been an issue in cloud federation[5], [9], and it can be seen in three dimensions: trust between consumer and CSP, between a CSP and other CSPs, and between a CSP and a CF. This study focuses on the data protection trust evaluation during the partner selection process for establishing a CF. According to previous research, the CSP's trust and data protection during the partner selection process can be evaluated from the CSP data policy alliance in alignment with the government data protection policy and strategy for the country, in which the data is physically located [4],[5].

Apart from trust, data privacy is another important factor to be considered in a cloud federation. Since various cloud providers own data centers located in different geographical locations, it allows the provider to offer services to their target audience in a particular region. Therefore, data location and relocation in CFs is the main concern, especially for a country that has restricted geographical location preferences. The international trade studies [10] and the strategic alliance domain studies [11] justify that partners' trust and country institutional quality (IQ) are mutually inclusive. The favorable impact of trust on commerce is conditional on IQ. Similarly, establishing a CF should favor the partner CSP's trustworthiness and the country's data protection capability. In existing cloud federation formation (CFF) strategies [4] [7]–[15], various types of trust sources, including SLA [21], [22], reputation [18], [21], [23] recommendation [20], feedback from users [11], [13], and peer providers [18], are utilized as a trusted source to measure the CSP's trustworthiness. However, the IQ, regulatory quality, and data protection strategies haven't been well-explored to be used as one of the CSP trust sources.

In General, considering trust evaluation and data confidentiality during the partner selection process is a significant stage in establishing reliable CF. Nonetheless, it is also the least-explored research area and this study aimed to fill this gap by providing a trust evaluation model considering data protection.

In section 2, related reviews are presented regarding the trust evaluation models in CF and show the previous research gap. Section 3 discussed the proposed trust evaluation model for data protection during the cloud federation formation. Section 4 presents the agent-based scenarios and simulation. Section 5 discussed the result of the simulation followed by a discussion and conclusion in section 6.

2 Literature Review

Trust evaluation has been explored through various studies and proposed different types of solutions to address trust in CFs through various dimensions. Trust is achieved through a process and is updated continuously in different stages. Moreover, the trust evaluation output of one stage will be the input for the next stage, and it continues in a round way that does not stop at a certain stage. Similarly, trust can be established in CFs through various CF stages, from partner selection until the end of the CF lifecycle. Through the procedure, determinants are used as input to the trust evaluation model to measure the trust level. A significant determinant used to evaluate the CSP trust level during the partner selection phase was explored in extensive studies. Muhammad et al. [12] have proposed a trust evaluation model that helps cloud service consumers to identify and select trustworthy CSPs. In the proposed evaluation model, CSP data from regulatory bodies, about CSP performance, and feedback from users were used as a trusted source, to identify the trusted CSPs. Ghafoorian et al. [24] proposed a direct and indirect trust evaluation model. The authors have addressed the reputation-based role-based access control and the accuracy requirements for the indirect trust model for storing the data storage cloud settings safely. Similarly, several determinants are used in research to be able to measure the CSP's trustworthiness. The prior widely used trust determinant is the previous experience [14], [17], [25]. The previous interactions incorporate the number of SLA violations [14], previous successful transactions [25], or the probability prediction of mistrust cost for different SLA parameters proposed by a CSP [17]. They are used as trust metrics for determining whether to cooperate again or interact with a new partner. Moreover, Naseer et al. [12] present a trust model that utilizes various parameters including downtime, uptime, SLA parameters, security measures, and data from regulatory bodies. The one-year transaction data accumulates in the regulatory bodies and this data is utilized to see the history of the CSP's success.

Furthermore, recommendations [12], [13], reputations [12], [14], or feedback [14]–[16] have been utilized in different studies as a determinant to evaluate trust with/without previous interaction parameters. Dhole et al. [12] present that previous interactions of CSP and recommendations are utilized to be able to learn about the CSP and to recommend it to another participant that does not have previous interactions. Moreover, Ahmed et al. [26] present the recommendation and feedback-based trust evaluation to establish CFs. It deals with excluding false feedback and recommendations by taking previous successful transactional history into consideration. Lastly, few studies use determinants like a recommendation, feedback, and reputation in addition to successful interactions. As an example, Mashayekhy et al. [14] propose a cloud federation formation mechanism utilizing previous interaction information, if it exists, or reputation, if the interaction history does not exist.

Overall, the literature review depicts that different determinants have been used as input to the trust evaluation model. It is clear that all these determinants address different dimensions to evaluate trust. However, the literature analysis also shows that trust regarding data protection is the least explored research area. Especially, the institution's trust level, along with the CSP trust, has not been examined, detailing where the data is physically located, the availability of data protection policy, and the government’s effectiveness. Therefore, this paper aimed to fill the gap in trust in data protection by

considering the governance indicators as an additional parameter along with feedback and reputation-based CSP trust.

3 Proposed Trust Evaluation Model

CF can be established within a country or across countries, considering different parameters [27], [28]. Among these parameters, trust is one of the main parameters to be evaluated. This study is focused on cross-bordered CF formation and proposes a trust evaluation model for selecting trusted partners during the CF establishment process. The overall trust (***Global Trust***) represents the institutional trust regarding data protection and the CSP trust. Therefore, this study divides the global trust into two: ***CSP Trust*** and ***Institutional Trust***. The CSP trust is an expectation about the candidate CSP that will react as expected. Institutional trust is the expectation about the country's rule of law, the readiness with regard to regulatory quality, data protection, related policy availability, and government effectiveness.

3.1 Model Description

Global Trust: As the effect of CSP trust in the presence of institutional trust wrt data protection is the main objective of this study, global trust is calculated as the mean of the CSP trust and institutional trust (equation 1)., and it is utilized during the partner selection of CFF.

$$Global\,Trust_i = mean\,(CSPTrust_i + InstitutionalTrust_i^{Country}) \quad (1)$$

Using this model, the trust of each provider i is calculated. The results are used for selecting trusted CSPs and establishing CF.

CSP Trust: The trust of a CSP is built on the satisfaction of peer CSPs that have experience with the focal CSP. Depending on the level of satisfaction, the peer CSPs express their opinion about the focal CSP i. The feedback from each peer CSP j is given by a value between 1 and 5. A value of 1 indicates the lowest feedback value, showing the peer CSP's dissatisfaction with the previous interaction with the focalCSP. A value of 5 indicates that the peer CSP is fully satisfied with the performance of the focal CSP.

$$AvgFeedback_i = \frac{\sum_{j=1}^{feedbackGiver_i} Feedback_i}{feedbackGiver_i} \quad (2)$$

The average feedback value, which is in the range between 1 and 5, is normalized as shown in equation 5, defining and measuring the CSP trust. Therefore, the CSP trust is in the range between 0 and 1. A value of 0 means that the CSP is not trusted, while a value of 1 represents that the CSP is trusted according to the recommendations given by the peer CSPs.

$$MaxAvgFeedback_i = 5 * feedbackGiver_i \quad (3)$$

$$MinAvgFeedback_i = feedbackGiver_i \quad (4)$$

$$CSPTrust_i = \frac{AvgFeedback_i - MinAvgFeedback_i}{MaxAvgFeedback_i - MinAvgFeedback_i} \quad (5)$$

where $MinAvgFeedback_i$ is the minimal feedback value, and $MaxAvgFeedback_i$ is the maximum feedback value in the survey.

Institutional Trust: Institutional trust is the other dimension addressed by the proposed model. It includes the country's rule of law, readiness with regard to regulatory quality, data protection policy availability, and government effectiveness. Institutional trust is measured through various parameters, but, for the sake of simplicity, we utilize the main 3 of them: namely data protection policy availability (PA) [29], policy quality (QA) [30], and cybersecurity in the country (CI) [31]. The variable PA measures the availability of data protection policy hence if the policy is available, the PA value will be 1 but if not the PA value will be 0. The QA is the quality of the available data protection policy and it is a subjective measure of the requester CSP depending on its policy preference. The last CI variable represents the national cybersecurity index with a value between 0 and 1. Depending on the weights given, the institutional trust of the trustee is calculated as shown in equation 6.

$$InstitutionalTrust_i^{Country} = \alpha_1 PA + \alpha_2 QA + \alpha_3 CI \text{ where } \alpha_1 + \alpha_2 + \alpha_3 = 1 \quad (6)$$

3.2 Cloud Federation Formation

Evaluating the proposed trust model is performed by utilizing the following CFF algorithm. In the algorithm, the *requester CSP* refers to the CSP who initiates the interaction to establish CF and the *peer CSPs* refer to the requested CSP to join the CF. The process of establishing CF consists of 12 main steps.

1. Create CSP ($PA, QA\ CI, Trust_{threshold}, Profit_i^{initial}$)
2. Calculate the initial trust of all CSP = Institutional trust
3. Requester CSP = choose random CSP
4. Requester CSP define $\alpha_1, \alpha_2, \alpha_3$
5. Requester CSP searches for peer CSPs
6. Is the peer CSPs global trust >= $Trust_{threshold}$
    a. If Yes go to step 3
    b. If No go to steps 7
7. Is requester CSP has a link with peer CSPs
    a. If Yes go to step 3
    b. If No go to steps 8
8. Requester CSP = get feedback ($Feedback_i$) from peer CSPs
9. Requester CSP update trust
    a. Calculate the CSP trust of peer CSPs using equation 5
    b. Calculate the Institutional trust of peer CSPs using equation 6
    c. Calculate the Global trust of peer CSPs using equation 1
10. Is Global Trust of peer CSPs >= $Trust_{threshold}$
    a. If yes go to step 10
    b. If No go to step 2
11. Create the link between requester CSP and peer CSPs (establish (join) CF)
12. Calculate the profit of CF and go to step 1

4 Simulation Model Scenario

The proposed model evaluation is performed by an agent-based modeling approach, utilizing the Netlogo simulation tool. In addition, it is assumed that the average feedback

is measured by an external system (feedback collector system). Therefore, only the outcome is used. Given this assumption, the following three scenarios are designed to evaluate the proposed model behavior:

Scenario 1 - High CSP trust with high institutional trust: This scenario aims to represent the CSP that delivers good service and gained high level of feedback with the availability of data protection policy, the quality of cyber security and a high index of cybersecurity. This kind of scenario represents a CSP that gave very good service to other peer providers and, therefore, gained a high level of feedback along with strong institutional trust.

Scenario 2 - High feedback rate with Low Institutional quality index: This scenario represents the CSP (data center) located in a low institutional quality country but still performs well and earned a high CSP trust level from its peer providers.

Scenario 3 - Low feedback rate with High Institutional quality index: In this scenario, a CSP, specifically a small-scale provider, could not obtain very good feedback from peers yet but operate in a high institutional trust environment. This CSP could not gain a high level of CSP trust, because it is new to the business, and it is challenging for them to compete with the current giant providers, preventing it from participating in a cloud federation.

Table 2. Simulation Setup and Configuration

Variable	Scenario-1	Scenario-2	Scenario-3
$Num_{feedbackGiver_i}$	100	100	100
$Feedback_i$	[3 … 5]	[3 … 5]	[1 … 3]
$max(feedback_{value})$	5	5	5
$min(feedback_{value})$	1	1	1
PA	1	0	1
QA	[0.5, 1]	[0, 0.5]	[0.5, 1]
CO	[0.5, 1]	[0, 0.5]	[0.5, 1]
$\alpha_1, \alpha_2, \alpha_3$	[0, 1]	[0, 1]	[0, 1]
$Trust_{threshold}$	0.5	0.5	0.5
$Profit_i^{initial}$	100	100	100

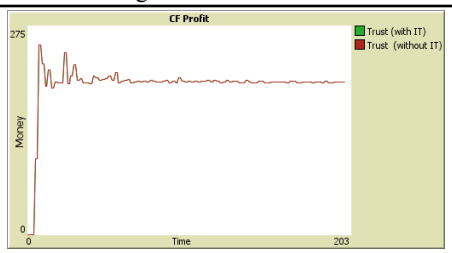
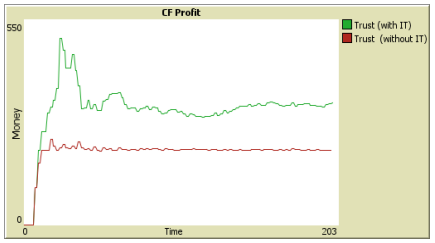
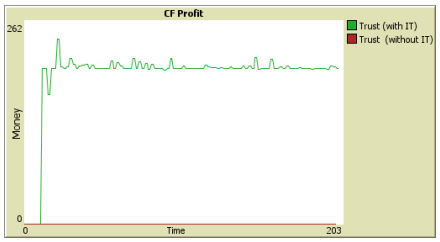
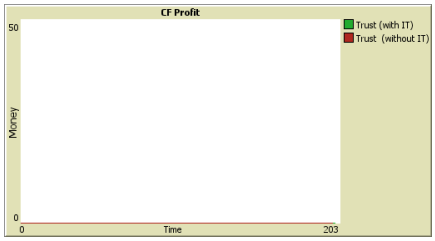
5 Result and Discussion

In a study from the International trade and strategic alliance domain area, it is justified that institution quality may produce trust or trust may substitute institutional quality. But in the cloud federation formation context, Institutional quality has not been considered in

order to select cloud service providers for the establishment of cloud federation. Therefore this paper aimed to fill this gap by considering institutional trust and CSP trust together by proposing a model.

For each scenario, the value given in table 1 is used in the proposed model. The proposed global trust model is compared with CSP trust without institutional trust. The simulation model is analyzed given three scenarios targeted by varying the level of feedback rate and institutional quality. The result shows that whenever the feedback rate and institutional quality are at a high level, the impact of CSP trust with or without institutional trust is similar. This shows that once the level of feedback rate is accumulated and achieved a high level, the effect of institutional quality is low. Therefore the CSPs which are located in the country with a high institutional quality index can be evaluated based on only their feedback rate level and establish cloud federation. However in this context, when the feedback-based trust is high while institutional quality is low or when the institutional quality of each CSP has a high index but their level of trust is low, the impact of institutional quality along with Trust is higher than only Trust. As shown in the result, the total profit of the established CF utilizing global trust is higher than that utilizing CSP trust. This shows that, in such a scenario, the uncertainty of institutional trust impacts the CF profitability. Therefore, the result tells that for the CSP located in a low institutional trusted country or for the CSP with a low trust level, the proposed model shows a positive impact on the CF.

Table 2. Simulation result

	High institutional trust	Low institutional trust
High Feedback		
Low Feedback		

CFF Stability favors profitability as one measurement parameter but it doesn't clearly show that profitability leads to CF stability. Business joint ventures measured their success by their profitability and to measure stability, partners' confidence level is a significant parameter to evaluate the business stability along with their profitability. Hence, in this paper, only profitability is addressed and further stability analysis is required as a further study. Therefore in the next plan, the confidence analysis will be evaluated with profitability and the CF stability will be analyzed.

6 Conclusion and Future Work

The study aimed to propose a trust evaluation model that investigates the CSP trust and institutional trust separately to calculate the global trust. The country's data protection status is an early prediction mechanism for future partners' trust in CF. Intended to this, the paper proposed and evaluate the CSP trust with and without the institutional trust

presence. The result shows that during low institutional trust with high CSP trust or low CSP trust with high institutional trust, the proposed model shows high profitability of the established CF network. Stability analysis needs further elaboration on the partner's conscience level. Therefore in future work, the authors will measure partners' confidence levels about the established CF network and stability will be analyzed.

Acknowledgment:

This research was supported by the BK21 FOUR (Fostering Outstanding Universities for Research) funded by the Ministry of Education (MOE, Korea) and the National Research Foundation of Korea (NRF). This work was also supported by the National Research Foundation of Korea (NRF) grant (No. NRF-2019R1F1A1058487) funded by the Ministry of Science and ICT (MSIT) of Korea.

References

[1] Z. Mahmood, "Data Location and Security Issues in Cloud Computing," in *2011 International Conference on Emerging Intelligent Data and Web Technologies*, Tirana, Albania, Sep. 2011, pp. 49–54. doi: 10.1109/EIDWT.2011.16.

[2] H. S. M. Abu-Nusair, "Data Location Compliance in Cloud Computing (Jordan Case Study)," M.C.S., Princess Sumaya University for Technology (Jordan), Jordan, 2013. Accessed: Aug. 15, 2022. [Online]. Available: https://www.proquest.com/docview/2570578478/abstract/28572B03CACB40E0PQ/1

[3] J. Noltes, "Data location compliance in cloud computing," Aug. 26, 2011. https://essay.utwente.nl/61042/ (accessed Aug. 15, 2022).

[4] Y. Gebrealif, M. Mubarkoot, J. Altmann, and B. Egger, "AI-Based Container Orchestration for Federated Cloud Environments," in *Proceedings of the 1st Workshop on Flexible Resource and Application Management on the Edge*, Virtual Event Sweden, Jun. 2020, pp. 15–16. doi: 10.1145/3452369.3463818.

[5] N. Haile and J. Altmann, "Risk-Benefit-Mediated Impact of Determinants on the Adoption of Cloud Federation," Seoul National University; Technology Management, Economics, and Policy …, 2015.

[6] R. Aryal, J. Marshall, and J. Altmann, "Architecture and Business Logic Specification for Dynamic Cloud Federations," 2019, pp. 83–96. doi: 10.1007/978-3-030-36027-6_8.

[7] A. Kanwal, R. Masood, and M. A. Shibli, "Evaluation and establishment of trust in cloud federation," 2014. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84899760598&doi=10.1145%2f2557977.2558023&partnerID=40&md5=37391e418deea959a3235e24dcd1ad10

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

[9] W. Mellaoui, R. Posso, Y. Gebrealif, E. Bock, J. Altmann, and H. Yoon, "Knowledge Management Framework for Cloud Federation," in *Economics of Grids, Clouds, Systems, and Services*, vol. 13072, K. Tserpes, J. Altmann, J. Á. Bañares, O. Agmon Ben-Yehuda, K. Djemame, V. Stankovski, and B. Tuffin, Eds. Cham: Springer International Publishing, 2021, pp. 123–132. doi: 10.1007/978-3-030-92916-9_10.

[10] S. Yu, S. Beugelsdijk, and J. de Haan, "Trade, trust and the rule of law," *European Journal of Political Economy*, vol. 37, pp. 102–115, Mar. 2015, doi: 10.1016/j.ejpoleco.2014.11.003.

[11] D. J. Kim, Y. I. Song, S. B. Braynov, and H. R. Rao, "A multidimensional trust formation model in B-to-C e-commerce: a conceptual framework and content analyses of academia/practitioner perspectives," *Decision Support Systems*, vol. 40, no. 2, pp. 143–165, Aug. 2005, doi: 10.1016/j.dss.2004.01.006.

[12] M. K. Naseer, S. Jabbar, and I. Zafar, "A novel trust model for selection of Cloud Service Provider," in *2014 World Symposium on Computer Applications & Research (WSCAR)*, Sousse, Tunisia, Jan. 2014, pp. 1–6. doi: 10.1109/WSCAR.2014.6916772.

[13] M. N. Derahman, A. Abdullah, and M. F. Azmi, "Robust reputation based trust management framework for federated-cloud environments," *International Journal of Applied Engineering Research*, 2016, [Online]. Available:

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85026679266&partnerID=40&md5=cd0a8910e1b1bc4e81a6e4f3a89677c8

[14] L. Mashayekhy, M. M. Nejad, and D. Grosu, "A Trust-Aware Mechanism for Cloud Federation Formation," *IEEE Trans. Cloud Comput.*, vol. 9, no. 4, pp. 1278–1292, Oct. 2021, doi: 10.1109/TCC.2019.2911831.

[15] K. Papadakis-Vlachopapadopoulos, R. S. González, I. Dimolitsas, D. Dechouniotis, A. J. Ferrer, and S. Papavassiliou, "Collaborative SLA and reputation-based trust management in cloud federations," *Future Generation Computer Systems*, vol. 100, pp. 498–512, Nov. 2019, doi: 10.1016/j.future.2019.05.030.

[16] M. K. Gupta and B. Annappa, "Trusted partner selection in broker based cloud federation," in *2016 International Conference on Next Generation Intelligent Systems (ICNGIS)*, 2016, pp. 1–6.

[17] S. Hadjres, F. Belqasmi, M. El Barachi, and N. Kara, "A green, energy, and trust-aware multi-objective cloud coalition formation approach," Future Generation Computer Systems, vol. 111, pp. 52–67, 2020.

[18] J. Abawajy, "Establishing trust in hybrid cloud computing environments," 2011. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84856193158&doi=10.1109%2fTrustCom.2011.18&partnerID=40&md5=1a68b3a35d726252e03d2f5597fccfb3

[19] B. Ray, A. Saha, S. Khatua, and S. Roy, "Quality and profit assured trusted cloud federation formation: Game theory based approach," IEEE Transactions on Services Computing, 2018.

[20] A. Dhole, M. V. Thomas, and K. Chandrasekaran, "An efficient trust-based Game-Theoretic approach for cloud federation formation," in 2016 3rd International Conference on Advanced Computing and Communication Systems (ICACCS), 2016, vol. 1, pp. 1–6.

[21] H. Kurdi, B. Alshayban, L. Altoaimy, and S. Alsalamah, "TrustyFeer: A Subjective Logic Trust Model for Smart City Peer-to-Peer Federated Clouds," Wireless Communications and Mobile Computing, 2018, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85044051077&doi=10.1155%2f2018%2f1073216&partnerID=40&md5=6b03461200de220697a740f9a23b12e0

[22] R. Latif, S. H. Afzaal, and S. Latif, "A novel cloud management framework for trust establishment and evaluation in a federated cloud environment," Journal of Supercomputing, 2021, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85104130905&doi=10.1007%2fs11227-021-03775-8&partnerID=40&md5=9352984d5a89e149390a2df92c88a34b

[23] U. Ahmed, I. Raza, and S. A. Hussain, "Trust evaluation in cross-cloud federation: Survey and requirement analysis," ACM Computing Surveys, vol. 52, no. 1. 2019. doi: 10.1145/3292499.

[24] M. Ghafoorian, D. Abbasinezhad-Mood, and H. Shakeri, "A Thorough Trust and Reputation Based RBAC Model for Secure Data Storage in the Cloud," IEEE Trans. Parallel Distrib. Syst., vol. 30, no. 4, pp. 778–788, Apr. 2019, doi: 10.1109/TPDS.2018.2870652.

[25] M. M. Hassan et al., "QoS and trust-aware coalition formation game in data-intensive cloud federations," Concurrency and computation: practice and experience, vol. 28, no. 10, pp. 2889–2905, 2016.

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

[27] R. G. Aryal and J. Altmann, "Dynamic application deployment in federations of clouds and edge resources using a multiobjective optimization AI algorithm," in 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC), Barcelona, Apr. 2018, pp. 147–154. doi: 10.1109/FMEC.2018.8364057.

[28] J. P. Romero Coronado and J. Altmann, Model for incentivizing cloud service federation. 2017. [Online]. Available: 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

[29] D. Hofman, L. Duranti, and E. How, "Trust in the Balance: Data Protection Laws as Tools for Privacy and Security in the Cloud," Algorithms, vol. 10, no. 2, p. 47, Apr. 2017, doi: 10.3390/a10020047.

[30] M. von Grafenstein, "Co-regulation and competitive advantage in the GDPR: Data protection certification mechanisms, codes of conduct and data protection-by-design,"

Research Handbook on Privacy and Data Protection Law, pp. 402–432, Mar. 2022.

[31] B. Krishna, S. Krishnan, and M. P. Sebastian, “Examining the Relationship between National Cybersecurity Commitment, Culture, and Digital Payment Usage: An Institutional Trust Theory Perspective,” Inf Syst Front, May 2022, doi: 10.1007/s10796-022-10280-7.