JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 10 Issue 02
2026

Research Article
https://doi.org/10.56979/1002/2026/1313

A Hybrid Trust Evaluation Framework for Cloud Service Providers in Cybersecurity-Critical Environments

Mamoon Obiedat[1], Ahmad Alkhatib[2], Qais Al-Na'amneh[3], Ayoub Alsarhan[1&4*], Mahmoud Aljawarneh[3], Rahaf Hazaymi[5], and Hussein Al-Ofeishat[6,7]

[1]Department of Information Technology, Faculty of Prince Al-Hussein Bin Abdallah II for Information Technology, The Hashemite University, Zarqa, Jordan.
[2]Cyber security department, Alzaytoonah university of Jordan, Jordan.
[3]Department of Cybersecurity and Cloud Computing, Applied Science Private University, Amman, Jordan.
[4]Department of Data Science and Artificial intelligence, Faculty of Information Technology, Al-Ahliyya Amman University, Amman, Jordan.
[5]Department of Computer Science, Jordan University of Science and Technology, Jordan.
[6]Department of Computer Science, Faculty of Information Technology, Al-Ahliyya Amman University, Amman, Jordan.
[7]Faculty of Engineering, Al-Balqa Applied University, Al-Salt, Jordan.
[*]Corresponding Author: Ayoub Alsarhan. Email: a.alsarhan@ammanu.edu.jo

Received: December 24, 2025 **Accepted:** February 27, 2026

Abstract: The rapid expansion of cloud computing has transformed digital service delivery, but establishing the trustworthiness of Cloud Service Providers (CSPs) remains a significant challenge, especially for sensitive workloads. This study presents a novel hybrid evaluation framework aimed at quantifying CSP trustworthiness from multiple perspectives. The framework combines a deterministic Multi-Attribute Trust Model (MATM) with a sophisticated Fuzzy Inference System (FIS). The MATM assesses CSPs based on three key attributes: Cost Efficiency (CE), Performance (P), and Reputation & Trustworthiness (RT). It utilizes a weighted normalization function to compute a transparent Trustworthiness Level (TL), offering a clear quantitative benchmark. To handle the inherent uncertainty and subjectivity in trust evaluation, the framework incorporates an FIS that uses fuzzy logic to interpret linguistic variables and capture the complex relationships among attributes. This dual approach provides both a straightforward, scalable assessment method and a more nuanced, human-centric evaluation. The framework's effectiveness was validated through scenario analysis. As an initial proof of concept, the evaluation utilized constructed provider scenarios representing typical market profiles. The results demonstrate the model's ability to clearly differentiate between service offerings, confirming its utility as a comprehensive decision-support tool.

Keywords: Cloud Computing; Trustworthiness; Multi-Attribute Trust Model; Fuzzy Logic; Cloud Service Provider; Reputation; Performance; Cost Efficiency

1. Introduction

The paradigm of cloud computing has fundamentally transformed the information technology landscape, establishing itself as the primary infrastructure for modern digital services [1], [2]. Its ability to deliver scalable, on-demand resources has driven innovation and improved operational agility. Despite these advantages, the widespread adoption of cloud computing is often hindered by a major challenge: the quantification and assurance of trustworthiness [3]–[5]. As organizations move critical operations to the cloud, the lack of direct control and the opaque nature of provider operations create a "trust deficit" [6]–[8]. This challenge spans multiple dimensions, including performance, cost, compliance, and reputation, which collectively inform the final Trustworthiness Level (TL) for CSP [9].

Traditional methods for evaluating CSPs typically focus on isolated metrics, such as Service Level Agreement (SLA) compliance or cost, offering an incomplete assessment [2], [10]. This fragmented evaluation process is inefficient and carries significant risks. A standardized, comprehensive, and quantitative framework is needed to holistically evaluate CSP trustworthiness from a multi-attribute perspective.

This research addresses this gap by proposing a Hybrid Trust Evaluation Framework (HyTEF). The framework combines a deterministic Multi-Attribute Trust Model (MATM) for clear scoring with a Fuzzy Inference System (FIS) to handle the ambiguity inherent in trust assessment [11]–[13]. This dual-methodology approach provides both a straightforward score and a nuanced analysis. This paper is structured as follows: Section II reviews related work. Section III details the methodology. Section IV presents results, and Section V concludes the paper.

2. Related Work

Establishing trust in cloud computing has been explored through various models, each focusing on different aspects such as SLA compliance and reputation systems. However, these traditional approaches have inherent limitations, highlighting the need for more comprehensive frameworks. This section reviews the most recent approaches for evaluating the trust level of CSPs.

2.1. SLA and Reputation-Based Models

Early approaches to evaluating trust in CSPs primarily focused on Service Level Agreements (SLAs) and reputation systems, both of which have notable limitations. Initial models relied on SLAs to establish contractual trust [3] and reputation systems that aggregate user feedback [14]. However, SLAs are reactive and limited in scope [15], while reputation systems are vulnerable to manipulation [16].

2.2. Multi-Attribute Decision-Making (MADM) Models

MADM methods like AHP and TOPSIS provide a more systematic framework for evaluating CSPs on multiple criteria [17], [18]. These models offer a structured approach [19], [20], but often require precise numerical inputs for qualitative attributes, which can be difficult to obtain.

2.3. Fuzzy Logic and AI-Based Models

Fuzzy logic-based models address uncertainty by utilizing linguistic variables, making them well-suited for trust evaluation [12], [21]–[23]. More recently, Artificial Intelligence (AI) and Machine Learning (ML) have been applied to dynamic threat detection and predictive analytics [24]–[27], [31-38]. However, these advanced models often suffer from high complexity and a "black box" issue, where their reasoning is not transparent [28].

2.4. Research Gap and Contribution

A gap remains for a hybrid framework that combines both the transparency of a weighted model and the nuance of a fuzzy system. The proposed Hybrid Trust Evaluation Framework (HyTEF) addresses this gap by synergistically integrating a Multi-Attribute Trust Model (MATM) for clear scoring with a FIS to manage ambiguity. A summary comparison is presented in Table 1.

Table 1. Comparative Summary of Related Work

Study/Author(s)	Methodology	Attributes	Limitations
Wenjuan et al. [3]	SLA Compliance	Uptime, etc.	Reactive
Xu et al. [14]	Reputation Sys.	User Ratings	Manipulable
Mishra et al. [17]	BWM-TOPSIS	QoS, Cost	Needs precise data
Mansour et al. [12]	Fuzzy Logic	SLA, Perf.	Complex rules
Butani et al. [24]	AI/ML	Threat patterns	"Black box" issue
Our Proposed HyTEF	**Hybrid**	**Cost, P, R**	**Balanced**

3. Methodology

Our methodology integrates a deterministic Multi-Attribute Trust Model (MATM) and FIS to evaluate the trustworthiness of CSPs based on key attributes such as CE, P, and RT. These attributes are calculated as follows:

Cost Efficiency (CE): Cost efficiency is a measure of how effectively a service or process utilizes its resources relative to its cost. It is evaluated by comparing the actual cost to a predefined range of acceptable costs, where a lower cost yields a higher score. In our work, it is computed as follows

$$f(CE) = \frac{C_{max} - C}{C_{max} - C_{min}} \quad (1)$$

where C_{max} maximum allowable or reference cost, C_{min} is minimum allowable or reference cost, and C is the actual cost being evaluated.

Performance (P): Performance refers to the operational effectiveness of a system, service, or process, often measured through factors such as uptime, throughput, and latency. It quantifies how well a system meets its intended goals and performs in real-world conditions. Higher performance typically corresponds to better system reliability and speed. It is computed as follows:

$$f(P) = \frac{(\text{Uptime} + \text{Throughput} + \text{Latency}^{-1})}{3} \quad (2)$$

where Uptime is the amount of time the system is operational and available for use, typically expressed as a percentage of total time, Throughput is the amount of data processed or handled by the system within a given period, often measured in transactions per second or data volume per second, and latency is the delay or response time between the input and output of the system, typically measured in milliseconds. In the equation, Latency is inversely related (i.e., lower latency improves performance), hence the Latency^{-1} term. This equation normalizes the performance by averaging these three components, where higher uptime, greater throughput, and lower latency lead to a better performance score

Reputation & Trustworthiness (RT): Measures a system's or service's credibility and reliability in the market, evaluating its standing based on security compliance, user feedback, and past incidents. A higher reputation and trustworthiness score reflect a more reliable and trusted service. In Equation 3, Reputation & Trustworthiness (RT) is calculated as:

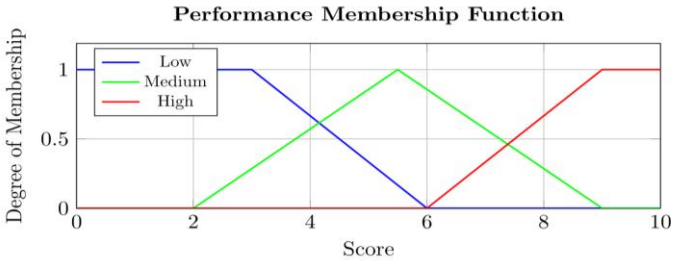
$$f(RT) = \frac{(S + R + C)}{3} \quad (3)$$

Where S Security Compliance [9], [29] indicates how well the system meets security standards and regulations, and R (User Ratings) [30] reflects the feedback and satisfaction levels from users and Incident Reports (C).

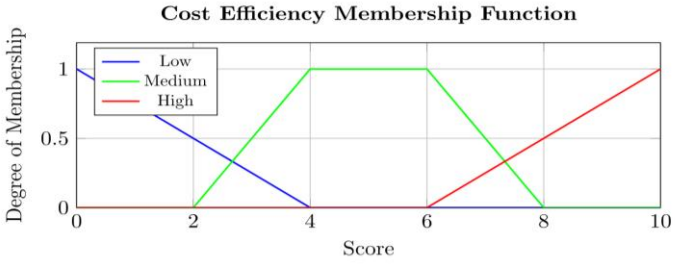
Each attribute is normalized to a $[0,1]$ scale. The final Trustworthiness Level (TL) is a weighted sum:

$$TL = w_1 \cdot f(CE) + w_2 \cdot f(P) + w_3 \cdot f(RT) \quad (4)$$

where $w_1 + w_2 + w_3 = 1$. (5)



(a) Performance Membership Functions



(b) Cost Efficiency Membership Functions

Figure 1. Membership functions for input attributes

The FIS handles vagueness by translating quantitative inputs into linguistic variables (Low, Medium, High) using membership functions, as shown in Fig. 1. Specifically, a Mamdani inference system is utilized,

employing a MIN operator for fuzzy intersection (AND) and a MAX operator for fuzzy union (OR). The rule base consists of 27 IF-THEN rules covering all combinations of the three attributes (e.g., "IF Cost Efficiency is High AND Performance is High AND Reputation is High, THEN Trust is Highly Trusted"). The output is converted to a crisp score using the Centroid defuzzification method, ensuring a transparent and reproducible mathematical translation from fuzzy sets to an actionable score.

3.1. Algorithmic Implementation

The overall process is summarized in Algorithm 1.

Algorithm 1 Trustworthiness Level Calculation

1: **Input:** CSP dataset with metrics
2: **Output:** Trustworthiness Level (TL) and Classification.
3: **Begin**
4: **for all** CSPs **do**
5: Calculate scores for CE, P, RT using (1)-(3).
6: Normalize CE, P, RT to a [0, 1] scale.
7: Assign weights (e.g., $w_1 = 0.33, w_2 = 0.34, w_3 = 0.33$ for equal importance).
8: $TL = w_1 f(CE) + w_2 f(P) + w_3 f(RT)$
9: **if** $TL > 0.8$ **then**
10: Classification ← "Highly"
11: **else if** $TL \geq 0.5$ **then**
12: Classification ← "Moderate"
13: **else**
14: Classification ← "Low"
15: **end if**
16: **end for**
17: **Output** CSP, TL, Classification.
18: **end**

The time complexity of the introduced algorithm can be analyzed based on the steps outlined in Algorithm 1. The algorithm processes a dataset of CSPs and computes the trustworthiness level (TL) for each CSP. For each CSP, the algorithm performs the following operations: calculating scores for CE, P, and RT (steps 5 and 6), normalizing the values (step 6), applying weights (step 7), computing TL (step 8), and classifying based on TL (steps 9-15). Assuming each of these operations takes constant time, the overall time complexity is dominated by the for-loop iterating over all CSPs. Let n be the number of CSPs in the dataset, the time complexity is $O(n)$, as the operations inside the loop are constant time operations. Therefore, the overall time complexity can be expressed as follows:

$$\text{Time Complexity} = O(n) \quad (6)$$

Where n is the number of CSPs in the dataset.

4. Results and Discussion

As an initial proof of concept, the framework was evaluated through scenario-based analyses rather than live provider data. In our study, we analyzed four CSP scenarios:

1) Premium (High P, High C, Strong R).
2) Budget (Low P, Low C, Mod R).
3) New Entrant (High P, Low C, Weak R).
4) Poor Value (Low P, High C, Weak R).

Table 2 shows the final scores assuming equal weighting. Fig. 2 visualizes the component scores.

Table 2. Comparative Analysis of CSP Scenarios

Scenario	Perf.	Cost	Rep.	Trust Score
High Perf, High Cost	High	High	Strong	High (0.65)
Low Perf, Low Cost	Low	Low	Moderate	Moderate (0.63)
High Perf, Low Cost	High	Low	Weak	Variable (0.55)
Low Perf, High Cost	Low	High	Weak	Low (0.23)

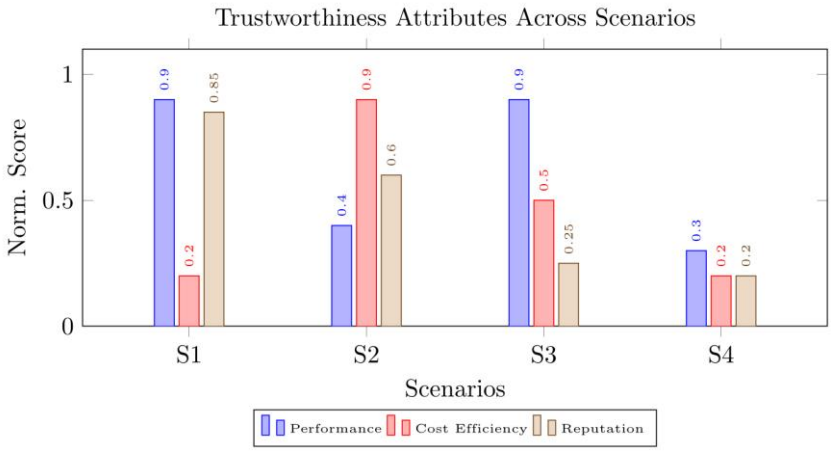


Figure 2. Normalized scores for scenarios S1-S4.

The figure illustrates the trustworthiness attributes—Performance, Cost Efficiency, and Reputation—across four distinct scenarios (S1, S2, S3, and S4). The normalized scores for each attribute were plotted, revealing a significant variation in the relative importance of these factors across different scenarios. In Scenario 1 (S1), the highest score was observed for Performance (0.9), while Cost Efficiency and Reputation were notably lower. A more balanced distribution was found in Scenario 2 (S2), where Performance and Reputation scored similarly high (0.85 and 0.6, respectively), with Cost Efficiency scoring 0.4. In Scenario 3 (S3), Reputation emerged as the most important factor, scoring 0.45, while Performance and Cost Efficiency remained low. Scenario 4 (S4) reflected a poor overall profile, with Performance, Cost Efficiency, and Reputation all remaining minimal (correlating with the "Poor Value" definition). Furthermore, as seen in Table 2, the non-linear scaling of the fuzzy inference system causes scenarios with mixed profiles (like S1 and S2) to yield closely clustered trust scores (0.65 vs 0.63). This occurs because the FIS rules severely penalize any single poor attribute (such as S1's high cost), bringing its overall trust score closer to a uniformly moderate provider (S2). This analysis highlights the dynamic nature of trustworthiness attributes in varying contexts, suggesting that the emphasis placed on each attribute depends on the specific scenario at hand.

4.1. Fuzzy Rule Surface Visualization

The 3D surface plots from the FIS visualize how Trustworthiness is influenced by Performance and Cost under different Reputation weights, as shown in Fig. 3. With a high reputation weight, the trust level has a high baseline. With a low weight, trust is primarily driven by performance and cost, and the overall trust level is constrained.

Fig. 3 presents a series of 3D plots that show the relationship between performance (Perf.), cost efficiency (Cost Eff.), and reputation weight across different reputation levels: high, medium, and low. These plots provide a visual understanding of how varying reputation weights influence the performance and cost efficiency trade-offs.

In the high reputation scenario (Fig. 3a), the relationship between performance and cost efficiency shows a steep positive trend, indicating that as cost efficiency improves, performance significantly increases. This suggests that entities with high reputations tend to balance both dimensions effectively, leading to better overall outcomes.

In contrast, the medium reputation scenario (Fig. 3b) reveals a more moderate slope. This indicates that for medium reputation entities, the impact of cost efficiency on performance is still positive but less pronounced than in the high reputation scenario. This implies a less efficient trade-off, where improving cost efficiency leads to performance gains, but the rate of improvement is slower.

Finally, in the low reputation scenario (Fig. 3c), the slope is much flatter, reflecting that performance gains due to improved cost efficiency are minimal. This suggests that entities with low reputations struggle to translate cost efficiency improvements into substantial performance gains, possibly due to external factors that overshadow cost-related decisions.

Overall, these plots highlight how reputation plays a crucial role in shaping the trade-offs between performance and cost efficiency. High reputation entities are able to leverage cost efficiency more

effectively to improve performance, while lower reputation entities face diminishing returns on performance despite improvements in cost efficiency.

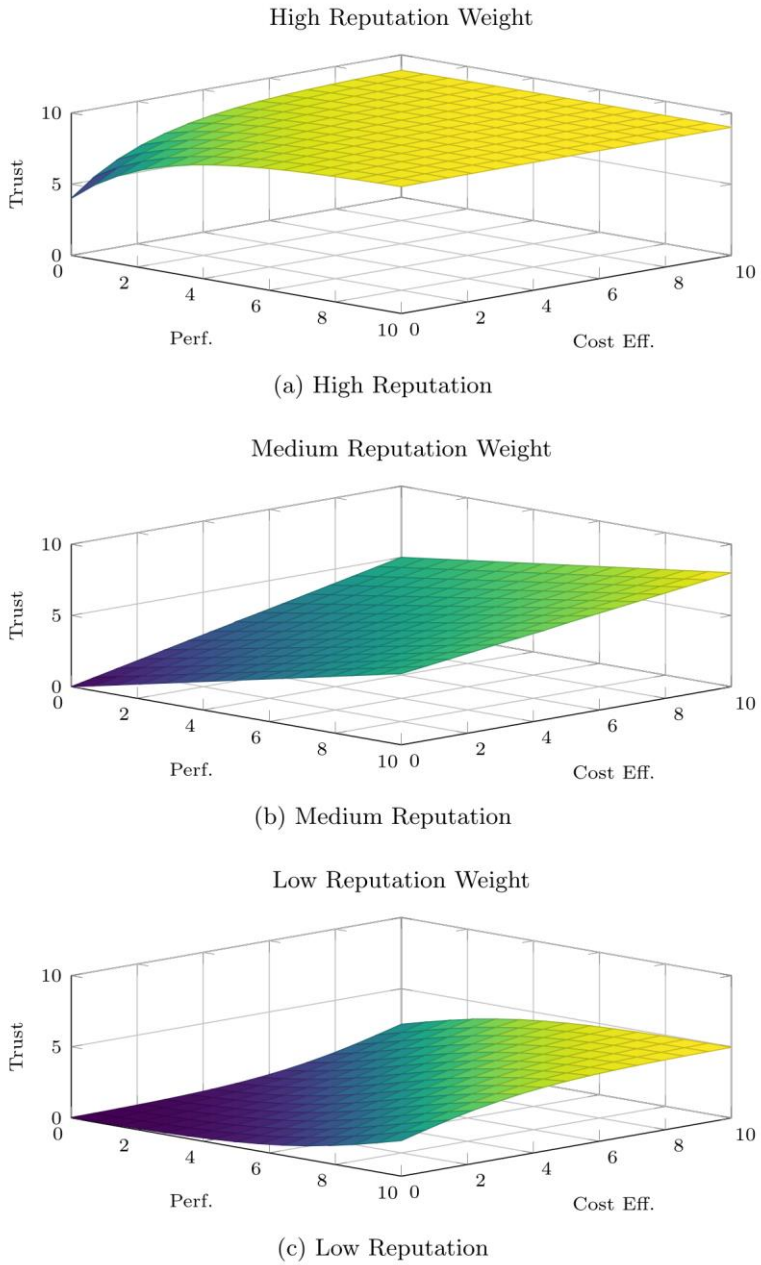


Figure 3. Trustworthiness surfaces under different reputation weightings.

The experiment in Fig. 4 compares client utilization between two schemes: Trust-based CSP selection (HyTEF) and Random CSP selection. This was generated via a simulated environment processing 1,000 iterative service requests, demonstrating the long-term decision value of the framework. In Scheme 1 (Trust-based CSP selection), clients choose CSPs based on a structured trust evaluation model, which incorporates Cost Efficiency (CE), Performance (P), and Reputation & Trustworthiness (RT). This model allows clients to select providers that offer the best balance of performance and cost, leading to higher engagement and utilization over time. The figure shows a steady increase in client utilization, suggesting that informed, trust-based decisions result in better service usage and client satisfaction.

In contrast, Scheme 2 (Random CSP selection), where clients randomly choose CSPs without evaluating key trust attributes, leads to slower and less consistent growth in client utilization. As the selection process is not based on performance, cost, or reputation, clients may encounter unsatisfactory service experiences, reducing their engagement. The figure highlights this inconsistency, confirming that trust-based selection models promote higher client utilization over time, as clients are more likely to stay with providers that meet their expectations for cost, performance, and reliability.

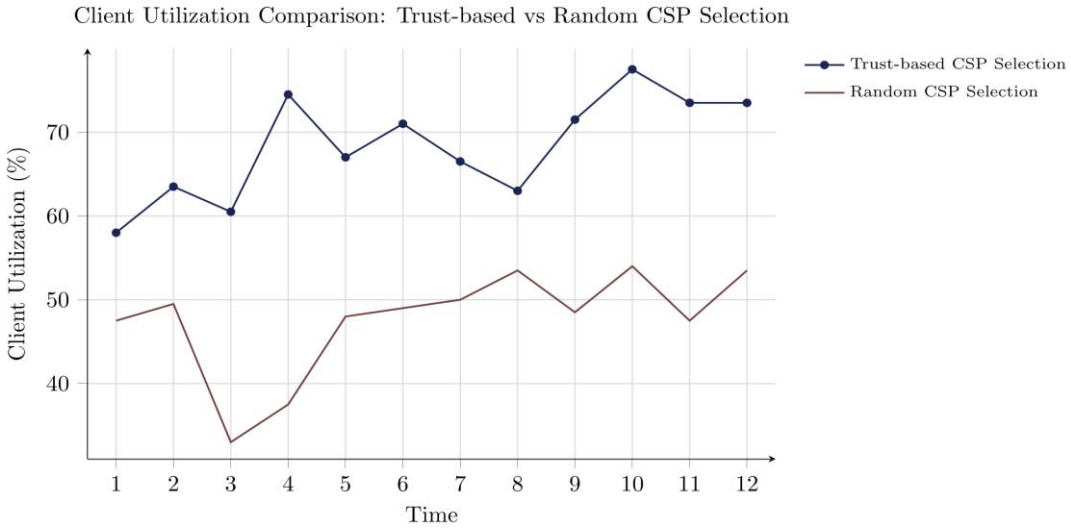


Figure 4. Comparison of Client Utilization: Trust-based CSP Selection vs. Random CSP Selection Over Time.

The HyTEF enforces a holistic evaluation, compelling decision-makers to consider the trade-offs between cost, performance, and reputation. The flexible weighting system allows for "what-if" analyses tailored to different stakeholder priorities. The fuzzy logic component incorporates qualitative expert opinions, resulting in a more robust and realistic assessment.

5. Conclusion and Future Work

This research presented a Hybrid Trust Evaluation Framework that integrates a deterministic MATM with an FIS. The framework provides a comprehensive, adaptable, and robust solution for assessing CSP trustworthiness, empowering enterprises to make more informed cloud adoption decisions.

Limitations include a dependency on reliable input data and the subjectivity in assigning weights. Future work will focus on integrating real-time data feeds and AI-driven anomaly detection to transform the framework into a continuous trust monitoring system [26], [27]. Further research could also explore additional attributes, such as data governance and sustainability metrics.

References

1. T. Alam, "Cloud computing and its role in the information technology," IAIC Transactions on Sustainable Digital Innovation (ITSDI), vol. 1, no. 2, pp. 108–115, 2020.
2. Q. Al-Na'amneh, M. Aljawarneh, R. Hazaymih, L. Alzboon, D. A. Laila, and S. Albawaneh, "Trust evaluation enhancing security in the cloud market based on trust framework using metric parameter selection," in Utilizing ai in network and mobile security for threat detection and prevention, IGI Global Scientific Publishing, 2025, pp. 233–254.
3. W. Li, J. Wu, J. Cao, N. Chen, Q. Zhang, and R. Buyya, "Blockchain-based trust management in cloud computing systems: A taxonomy, review and future directions," Journal of Cloud Computing, vol. 10, no. 1, p. 35, 2021.
4. A. A and S. K. E, "Development of trustworthiness for cloud service providers using DBN-based trust model in cloud computing environment," International Journal of Human–Computer Interaction, vol. 41, no. 8, pp. 4583–4593, 2025.
5. J. Sidhu and S. Singh, "Improved TOPSIS method based trust evaluation framework for determining trustworthiness of cloud service providers," Journal of Grid Computing, vol. 15, pp. 81–105, 2017.
6. P. Goyal and S. S. Deora, "A comprehensive survey on trust management in cloud computing," International Journal of Computer Networks and Applications, vol. 9, no. 6, pp. 761–774, 2022.
7. Q. Al-Na'amneh, R. Hazaymih, M. A. Almaiah, and L. Alzboon, "Secure cloud-marketplaces: A trust framework for evaluating security for client service providers," in Utilizing AI in network and mobile security for threat detection and prevention, IGI Global Scientific Publishing, 2025, pp. 255–280.
8. X. Wu, R. Zhang, B. Zeng, and S. Zhou, "A trust evaluation model for cloud computing," Procedia Computer Science, vol. 17, pp. 1170–1177, Dec. 2013.
9. A. O. Akinade, P. A. Adepoju, A. B. Ige, and A. I. Afolabi, "Cloud security challenges and solutions: A review of current best practices," Int J Multidiscip Res Growth Eval, vol. 6, no. 1, pp. 26–35, 2025.
10. A. Selvaraj and S. Sundararajan, "Dynamic multi attribute trust evaluation system for IaaS services," International Journal of Applied Science and Engineering, vol. 17, no. 1, pp. 1–10, 2020.
11. Y. Singh and D. C. Bisht, "Enhanced dissimilarity measurement for pythagorean fuzzy sets in real-world scenarios," International Journal of System Assurance Engineering and Management, vol. 16, no. 1, pp. 402–424, 2025.
12. B. M. M. Mansour, T. Abdelkader, M. Hashem, and E. M. El-Horbaty, "An integrated three-tier trust management framework in mobile edge computing using fuzzy logic," PeerJ Computer Science, vol. 7, p. e700, 2021.
13. Q. Al-Na'amneh, A. Alsarhan, M. Aljawarneh, A. S. Alhazaimeh, A. Alzoubi, and R. Hazaymih, "Security approach to identify client trust values (CTV) in the cloud market by using fuzzy logic inference system," in Blockchain detection of cybersecurity attacks and risk management, IGI Global Scientific Publishing, 2026, pp. 161–182.
14. J. Xu, D. Jiang, B. Wang, D. Yang, and S. Reiff-Marganiec, "Local reputation management in cloud computing," in 2015 IEEE world congress on services, 2015, pp. 261–267.
15. B. A. Alenizi, M. Humayun, and N. Jhanjhi, "Security and privacy issues in cloud computing," Journal of Physics: Conference Series, vol. 1979, no. 1, p. 012038, Aug. 2021.
16. Q. Wu, X. Zhang, M. Zhang, Y. Lou, R. Zheng, and W. Wei, "Reputation revision method for selecting cloud services based on prior knowledge and a market mechanism," TheScientificWorldJournal, vol. 2014, p. 617087, Feb. 2014.
17. A. Mishra and R. Kumar, "Ranking of cloud services by applying bwm-topsis, bwm-aras, and bwm-copras hybrid mcdm methods," International Journal of Data Science and Analytics, vol. 20, no. 6, pp. 5301–5319, 2025.
18. 18. S. Jaiswal and A. Mishra, "Cloud service selection using TOPSIS and Fuzzy TOPSIS with AHP and ANP," International Journal of Computer Applications, vol. 167, pp. 22–28, 2017.
19. S. U. Khan, H. U. Khan, N. Ullah, and R. A. Khan, "Challenges and their practices in adoption of hybrid cloud computing: An analytical hierarchy approach," Security and Communication Networks, vol. 2021, no. 1, p. 1024139.
20. M. Z. Khan, M. Shoaib, M. S. Husain, K. Ul Nisa, and Mohammad. T. Quasim, "Enhanced mechanism to prioritize the cloud data privacy factors using AHP and topsis: A hybrid approach," Journal of Cloud Computing, vol. 13, no. 1, Feb. 2024.
21. I. R. Sekhi, H. Abdah, and K. Nehéz, "Reliable and cost-effective fuzzy-based cloud broker," International Journal of Networked and Distributed Computing, vol. 13, p. 10, 2025.
22. M. Faiz and A. K. Daniel, "A multi-criteria cloud selection model based on fuzzy logic technique for QoS," International Journal of System Assurance Engineering and Management, vol. 15, no. 2, pp. 687–704, 2024.

23. J. Ahmmad, H. El-Wahed Khalifa, H. M. Waqas, A. Alburaikan, and T. Radwan, "Ranking data privacy techniques in cloud computing based on tamir's complex fuzzy schweizer-sklar aggregation approach," Scientific Reports, vol. 15, no. 1, p. 24943, 2025.
24. J. B. Butani, "AI-based zero trust security models for cloud computing," in AI and digital transformation: Opportunities, challenges, and emerging threats in technology, business, and security, 2026, pp. 509–518.
25. I. E. Berna, K. Vijay, S. Gnanavel, and J. Jeyalakshmi, "Impact of artificial intelligence and machine learning in cloud security," in Improving security, privacy, and trust in cloud computing, IGI Global Scientific Publishing, 2024, pp. 34–58.
26. A. A. Mehdi Syed and E. Anazagasty, "AI-driven infrastructure automation: Leveraging AI and ML for self-healing and auto-scaling cloud environments," International Journal of Artificial Intelligence, Data Science, and Machine Learning, vol. 5, pp. 32–43, 2024.
27. R. C. Thota, "AI-augmented predictive analytics for proactive cloud infrastructure management," Journal of Science & Technology, vol. 5, no. 4, pp. 246–264, 2024.
28. M. Akbar, M. M. Waseem, S. H. Mehanoor, and P. Barmavatu, "Blockchain-based cyber-security trust model with multi-risk protection scheme for secure data transmission in cloud computing," Cluster Computing, vol. 27, no. 7, pp. 9091–9105, Apr. 2024.
29. L. Badger, D. Bernstein, R. B. Bohn, F. J. de Vaulx, M. D. Hogan, M. Iorga, J. Mao, J. Messina, K. Mills, E. Simmon, A. Sokol, J. Tong, F. Whiteside, and D. Leaf, "US government cloud computing technology roadmap, special publication 500-293," National Institute of Standards; Technology, Gaithersburg, MD, USA, Special Publication 500-293, 2014.
30. S. Ganesh, "Key takeaways from the 2024 gartner cloud security report on CNAPP." https://blog.qualys.com/product-tech/2024/08/14/our-takeaways-from-2024-gartner-market-guide-for-cloud-native-application-protection-platforms-cnapp-insights-and-market-evolution, 2025.
31. Al-Na'amneh, Qais, Aljaidi, Mohammad, Nasayreh, Ahmad, Gharaibeh, Hasan, Al Mamlook, Rabia Emhamed, Jaradat, Ameera S., Alsarhan, Ayoub and Samara, Ghassan. "Enhancing IoT device security: CNN-SVM hybrid approach for real-time detection of DoS and DDoS attacks" Journal of Intelligent Systems, vol. 33, no. 1, 2024, pp. 20230150. https://doi.org/10.1515/jisys-2023-0150.
32. Shalaldeh, A., Abualhaj, M., Abu-Shareha, A. A., Elshenawy, A., Saoudi, Y., Hussain, M., ... & Logan, C. (2026). Designing Predictive Models: A Comparative Evaluation of Machine Learning Algorithms for Predicting Body Carcass Fat in Ewes at Weaning. Agriculture, 16(4), 488.
33. Almaini, A., Al-Dubai, A., Romdhani, I., Schramm, M., & Alsarhan, A. (2021). Lightweight edge authentication for software defined networks. Computing, 103(2), 291-311.
34. Alhijawi, B., Kilani, Y., & Alsarhan, A. (2020). Improving recommendation quality and performance of genetic-based recommender system. International Journal of Advanced Intelligence Paradigms, 15(1), 77-88.
35. Aljaidi, M., Samara, G., Singla, M. K., Alsarhan, A., Hassan, M., Safaraliev, M., ... & Tavlintsev, A. (2024). A particle swarm optimizer-based optimization approach for locating electric vehicles charging stations in smart cities. International Journal of Hydrogen Energy, 87, 1047-1055.
36. Almalkawi, I. T., Halloush, R., Alsarhan, A., Al-Dubai, A., & Al-Karaki, J. N. (2019). A lightweight and efficient digital image encryption using hybrid chaotic systems for wireless network applications. Journal of Information Security and Applications, 49, 102384.
37. M. M. Abualhaj, M. O. Hiari, A. Alsaaidah, and M. M. Al-Zyoud, "Comparative analysis of whale and Harris Hawks optimization for feature selection in intrusion detection," Indonesian Journal of Electrical Engineering and Computer Science, vol. 37, no. 1, p. 179, Jan. 2025, doi: https://doi.org/10.11591/ijeecs.v37.i1.pp179-185.
38. Aljaidi, M., Alsarhan, A., Samara, G., AL-Khassawneh, Y. A., Al-Gumaei, Y. A., Aljawawdeh, H., & Alqammaz, A. (2022, November). A critical evaluation of a recent cybersecurity attack on itunes software updater. In 2022 International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICEEAI) (pp. 1-6). IEEE.