International Journal of Basic and Applied Sciences, 14 (3) (2025) 258-265

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/vbn70d23
Research paper

Comparative Analysis of Trust-Based Data Storage Management Techniques in Dynamic Cloud Service

K. H. Vani [1] *, Dr. P Balamurugan [2]

[1] Assistant professor, Department of Computing, Coimbatore Institute of Technology, Coimbatore, Tamilnadu- 641014
[2] Associate professor, Department of Computer Science, Government Arts College (Autonomous), Gopalapuram, Coimbatore, Tamil Nadu 641018
**Corresponding author E-mail: vanikhassistantprofessor@gmail.com*

Received: June 12, 2025, Accepted: July 14, 2025, Published: July 24, 2025

Abstract

Cloud computing (CC) has emerged as a transformative paradigm for data storage and service delivery. However, challenges in trust management, data confidentiality, and quality assurance continue to limit its scalability and user adoption. To address these limitations, this study proposes a Triple-layered Trust Evaluation Model (TTEM) that integrates trust computation, optimized cryptographic key generation, and a layered architecture comprising edge, fog, and cloud nodes. The model dynamically evaluates service providers based on multiple Quality of Service (QoS) attributes—such as bandwidth, memory, cost, and reliability—using a user satisfaction score computed through weighted aggregation. Trust values are calculated at the fog layer to reduce latency and ensure scalability, while secure session keys are generated using a metaheuristic-based optimizer for robust cryptographic protection. The proposed TTEM is simulated and evaluated using real-world multi-cloud scenarios, including datasets from Google Drive, PCloud, MEGA, and MediaFire. Comparative results show that TTEM outperforms existing methods such as GA, CSA, and MSFOA in terms of trustworthiness, computational efficiency, resource utilization, and data security. The model is particularly suited for dynamic, privacy-sensitive applications in smart cities, healthcare, and industrial IoT environments.

Keywords: *Trust Evaluation Model; Multi-Cloud Storage; Fog Computing; Edge Computing; Cryptographic Key Optimization; Cloud Security; Quality of Service (QoS); Privacy Preservation; Trust Management; Distributed Architecture.*

1. Introduction

A cloud service is a group of computing resources, typically referring to a scalable and dynamic virtualized resource that includes services such as storage, computing, and application services. On the one hand, different CSPs can offer identical cloud services; on the other hand, their qualities range greatly. With the expansion of CC, customers will face an increasingly crucial problem: many CSPs must select the best cloud services [1]. The quality of CS is a significant factor influencing the growth of CC. There are numerous trust evaluating techniques that can be employed to assess the secure storage, QoS transactions, cloud service security, cloud manufacturing, and so on [2]. Despite its broad acceptance, CC challenges to meet the bandwidth and latency imply of Internet of Things (IoT) applications, prompting the use of fog and edge computing to supplement cloud capabilities [3]. These prototypes address latency and bandwidth issues by bringing computing nearer to data at the network's edge, while also encouraging a cooperating dynamic among three layers. In this teamwork, the device-boosted edge paradigm allows IoT devices to use their idle processing resources. This strategy not only lightens the pressure on standard edge servers, but it also encourages flexibility and resource efficiency. However, using a cooperative device-enhanced edge-fog-cloud infrastructure has significant difficulties, involving assignment of jobs over diverse resources and changing node availability, and sustaining QoS [4].
The edge-fog-cloud topology is usually known as a triple-layered model. The edge layer is located at the bottom and links to end-user IoT devices directly. The cloud layer is located at the top, and the middle tier is made up of fog nodes, as illustrated in Figure 1. The triple-layer interaction can occur through different assessments, but it adheres to the model in [5]. To address the high throughput and QoS demands of terminal IoT edge nodes while ensuring cost efficiency, an IoT-edge-based fog arrangement is proposed. This model incorporates essential elements such as system coverage, architecture, network connectivity, and their challenges related to multi-objective fog node deployment. The edge tier or IoT-edge tier (first tier) consists of numerous IoT-edge terminal nodes that connect to the second one, termed the fog tier, which contains multi-fog server nodes. The next one (third) is the cloud layer, in which computing nodes can execute intensive data analytics chores.

Copyright © K. H. Vani, Dr. P Balamurugan. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The trustworthiness of any CSP is critical for mitigating risks, protecting data maintained with CSPs, ensuring service quality, and verifying compliance with regulatory requirements, among other things. Trust is divided into two types: subjective trust, in which the user applies his interests to interactions, and objective trust, which is based only on individuals' interacting experiences.

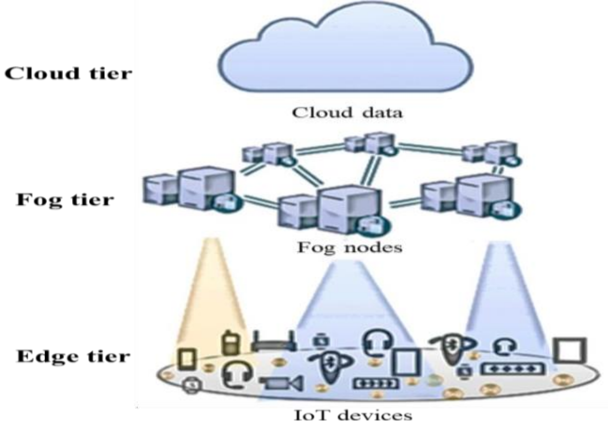

Fig. 1: IoT-Edge-Based Fog Arrangement.

Several corporations and organizations have recently been driven by their intention to possess a big capacity for storage with efficient scalability, and small businesses, when migrating to the triple-layer, containing those prototypes from standalone execution. Significantly, this transformation will provide various hurdles along the way. The submitted work provides attention on how to establish security in these triple-layer computing systems while protecting users' privacy from attackers [6]. Fundamentally, the idea is a comprehensive managing approach for personal data that hosts these layers at global centres. The concept of a group of end-user IoT systems collectively operating as a collective work-out resource has been examined in several studies, including many titles like mobile device clouds [7].

Security and privacy concerns have grown in importance as customers receive large volumes of data and crucial software from cloud providers [8]. Because of these concerns, related topics provide significant hurdles to the computing paradigms study field. Presently, the primary focus of every computing paradigm is on protecting users' privacy from unwanted groups or persons gaining access and preventing assaults. Furthermore, ensuring data integrity is an extremely important component. This submitted research examines the security and privacy issues of the triple-layer paradigms. The goal of this study is to provide a simple and optimized trust evaluation structure for cloud-based services. In the study, a new triple-layer architecture with an optimized cryptographic model is proposed in which IoT devices function as edge resource providers.

- To connect fog nodes efficiently and encompass all edge nodes, a multi-objective function is projected that aims to maximize the coverage of edge devices while enhancing network connectivity.
- To ensure seamless connectivity and comprehensive connectivity for every device and fog nodes, hence boosting entire network reliability and ensuring QoS.
- To introduce an optimized cryptographic key generating model is designed to exploit network connectivity and coverage.
- To facilitate effortless estimation, the proposed approach has been developed and evaluated across different network configurations.
- To analyse how various parameters affect network functionality and determine the most efficient optimization techniques.
- To indicate the outcomes with a substantial enhancement in both connectivity and coverage compared to existing methods.

The related reviews, overall methodological concept, submitted idea in the scheme, simulation evaluation, and its conclusions are given one by one in the following.

2. Literature survey

In recent years, researchers have raised significant concerns about data privacy and security within cloud computing ecosystems. As cloud adoption expands, users and organizations increasingly relinquish direct control over their data, exposing it to potential breaches and unauthorized access. Raja (2024) explores these emerging risks, emphasizing how the shift to virtualized, remote environments has introduced complex data management challenges that traditional security methods can no longer adequately address [9]. To counter these limitations, trust evaluation models are being actively developed. One such method is based on fuzzy logic, which allows for flexible, human-like reasoning in assessing cloud service trustworthiness. John and Singh (2024) proposed a fuzzy inference-based analytical process that evaluates cloud service providers by integrating multiple variables, such as user satisfaction, service consistency, and reliability scores [10]. Their model supports a more adaptable and personalized assessment of trust compared to rigid numerical metrics.

Further advancing the user-oriented perspective, Balcão-Filho et al. (2021) designed a consumer-centric framework that empowers end-users to evaluate trust based on their expectations and interactions with cloud services. Their study underscores the importance of aligning trust evaluation with user-defined parameters rather than generic benchmarks, facilitating a more accurate and meaningful assessment process [11]. In addition to soft computing approaches, blockchain technologies have emerged as powerful tools for decentralized trust management. Li et al. (2024) introduced a blockchain-based trust system tailored for vehicular ad hoc networks (VANETs), which safeguards user location privacy while ensuring data authenticity. By leveraging blockchain's tamper-resistant structure, their model establishes verifiable trust relationships without relying on centralized authorities [12].

Privacy-preserving architectures have also been explored for cloud-based persistent computations. Chen et al. (2024) proposed a dual-cloud multi-secret sharing framework, which splits sensitive data into encrypted segments distributed across different clouds. This architecture reduces the risk of single-point data leakage and ensures computational integrity, especially in long-term storage scenarios [13]. To further optimize privacy in cloud systems, Sugitha and S. (2024) presented a multi-objective model based on the hunter-prey optimization (HPO) algorithm. Their method dynamically adjusts privacy controls based on data classification and user requirements, offering a scalable solution for real-time privacy enforcement across diverse cloud environments [14]. The current developments in trust modeling do indicate a large range of approaches. John and Singh (2024) used a fuzzy inference system, which combines several parameters determined by the user to determine reliability of Cloud Service Providers (CSPs). This method of soft computing can handle subjectivity, and it lends itself to individualized trust estimations. By comparison, Li et al. (2024) introduced a blockchain-based trust model of VANETs with a tamper-proof record-keeping system and decentralized control, with an emphasis on data integrity rather than flexibility. The proposed TTEM model will span between these paradigms: it will operate on adaptable scoring, which is based on user satisfaction indicators and incorporate the features of session-based security using streamlined cryptographic key management, thereby being both adaptable and robust. Furthermore, the new meta heuristic has performed better in dynamic allocation of resources and security. This category comprises most recent models like hybrid GA-CSA, entropy-enhanced swarm optimization, and hunter-prey algorithm (Sugitha & S, 2024). The state-of-the-art is that TTEM is an extension of the Modified Sooty Tern Optimization Algorithm (MSFOA) that proposes adaptive seeding, as well as entropy modulation, in the improved sequence.

In parallel, attention has shifted toward the structural integration of edge, fog, and cloud computing—especially in IoT scenarios where latency and context awareness are critical. Firouzi et al. (2022) explored how fog and edge computing layers act as intermediaries between cloud infrastructure and IoT devices. Their research demonstrates that processing data closer to its origin can reduce latency, energy consumption, and data traffic, enabling more responsive applications [15]. Security and resilience concerns within this triple-layered architecture were discussed by Shirazi et al. (2017), who conducted an in-depth analysis of the vulnerabilities in mobile edge computing and fog networks. Their findings point to the need for decentralized yet robust security frameworks that can operate in resource-constrained environments [16]. Wang et al. (2017) broadened this perspective by surveying mobile edge networks that combine computing, caching, and communication functionalities. Their study highlights the potential for these converged networks to deliver low-latency services while minimizing the burden on centralized cloud data centers [17]. Ren et al. (2019) further investigated collaborative computing models where edge and cloud systems work together to reduce latency. Their work focuses on task offloading strategies that intelligently delegate workloads based on proximity and processing capability, thus improving system responsiveness for real-time and mission-critical applications [18].

Collectively, these studies contribute valuable insights into trust computation, privacy preservation, and performance optimization in cloud and edge environments. They serve as foundational elements for the development of secure, trust-aware architectures like the proposed Triple-layered Trust Evaluation Model (TTEM), which integrates cryptographic, infrastructural, and behavioral trust mechanisms to enhance cloud storage reliability. Overall, the literature establishes the need for secure, trust-aware, and performance-optimized models in multi-cloud environments—validating the proposed Triple-layered Trust Evaluation Model (TTEM) in your study.

3. Methodological framework and system architecture

This section outlines the foundational structure of the proposed Triple-layered Trust Evaluation Model (TTEM), detailing the interactions across edge, fog, and cloud layers. It presents key architectural components, user and system entities, computational parameters, and the trust evaluation methodology integrated with optimized cryptographic key generation. Establishing trust in a triple-layer environment (Figure 2) is a significant challenge, particularly as numerous applications handle sensitive data. Those critical requirements drive the need to develop a load-balanced, trust-enforced environment for reliable applications, aimed at minimizing response times. The succeeding subsections will provide a detailed background and motivation for this initiative [19].

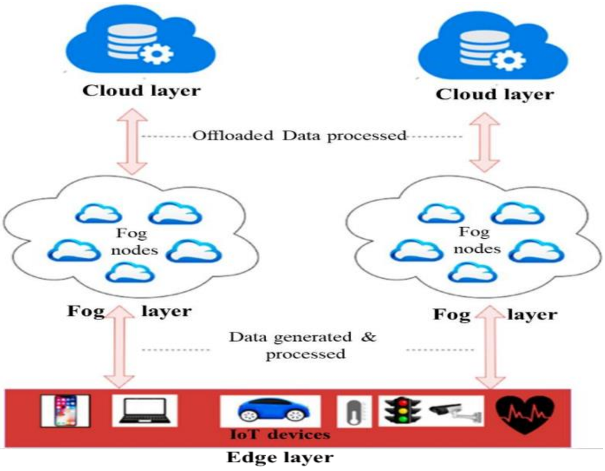

Fig. 2: Triple-Layer with Multi-Cloud System.

This primary layer generates and transmits data to the preceding level. It comprises a wide array of diverse IoT devices, such as mobile devices and wearable sensors, which play a crucial role in data generation. These devices communicate with the Fog layer using popular communication protocols like Bluetooth or other connecting technologies. The generated data is sent to the resource-rich Fog environment for processing and analysis. This layer seems more versatile than the earlier one, with multiple distributed nodes spread across various vendor-specific sites. Each Fog node is outfitted with processing power, data storage, and communication capabilities. The principal function of this level layer serves to evaluate data acquired from IoT devices, incorporating its capabilities to promote efficiency. FC is applied to promote the functionality of IoT services because of lessening request-response times over latency-sensitive applications and thereby lessening the communication and processing burden on the cloud. Fog nodes act as a bridge across IoT devices and the cloud.

This is the topmost layer in the architecture, facilitating efficient access to cloud resources. The cloud layer is significantly more resourceful than the Fog layer, capable of handling large-scale data processing and computations that exceed the capabilities of the Fog layer.

The number of IoT devices and applications is growing exponentially. However, these devices often struggle with computationally and storage-intensive tasks due to their limited resources, necessitating task offloading. Typically, these tasks are offloaded to cloud services, whether public or private. A significant challenge with cloud services is latency, which can arise from distance and bandwidth constraints. FC addresses this issue by delivering services closer to the user, at the edge of the network. It extends cloud computing by providing computation, storage, and networking services directly at the end device. However, many applications running on IoT devices today are trusted applications that handle sensitive data. This sensitive data can be well-secured using a better key optimization scheme. The complete trust model is described in the next section.

4. Proposed model: triple-layered trust evaluation model (TTEM)

Cloud computing has become integral to modern digital ecosystems, especially in sectors requiring high security and reliability such as healthcare, finance, and smart cities. However, ensuring the confidentiality, integrity, and trustworthiness of data shared across distributed platforms remains a persistent challenge. To address this, a novel Triple-layered Trust Evaluation Model (TTEM) is proposed. This model integrates a hierarchical computing structure, dynamic trust evaluation, and optimized cryptographic key management to enhance cloud service security and performance in multi-cloud settings. The TTEM architecture is built on a layered approach, comprising the Edge, Fog, and Cloud tiers. The edge layer, consisting of various IoT and mobile devices, is responsible for generating data and initiating service requests [20]. These devices often have limited resources and thus require efficient offloading strategies. The fog layer acts as a middle layer that bridges edge devices and cloud infrastructure. It is equipped with greater computational power and handles tasks like intermediate processing, trust aggregation, and session management. The cloud layer, being the most resource-rich, performs data-intensive operations and stores large-scale data securely. This layered topology ensures reduced latency, scalability, and efficient processing across distributed systems.

The model includes multiple system entities that collaborate within the TTEM framework. Cloud Service Providers (CSPs) offer cloud-based infrastructure and storage services, while Cloud Service Users (CSUs) utilize these services through their Edge Devices (EDs) such as sensors and mobile nodes. Fog Nodes (FNs) are strategically placed intermediate processors that manage network load and facilitate fast response. Each fog node governs a Fog Computing Domain (FCD) and may elect a Trust Coordinator, which evaluates the behavior of its associated edge nodes. This coordination minimizes redundant trust computations and enhances the scalability of the system. Mutual authentication protocols are enforced between all interacting components to ensure a secure and trusted environment. At the core of TTEM lies a real-time trust evaluation mechanism that quantitatively assesses service quality using multiple parameters such as bandwidth, memory availability, cost, and reliability. Each service request is evaluated based on the user's expectations versus actual performance. A weighted aggregate of these parameters provides the user satisfaction score. The overall trust value is derived by averaging satisfaction scores across multiple services, enabling dynamic updates to trust ratings. This adaptive model ensures that trust scores remain accurate and reflect current CSP behavior, thereby supporting secure and informed service selection by users.

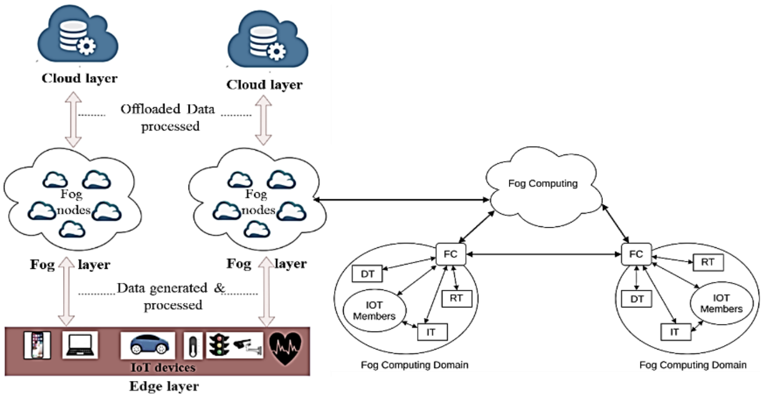

Fig. 3: System Architecture of the Proposed Triple-Layered Trust Evaluation Model (TTEM).

To guarantee data security and prevent unauthorized access, TTEM integrates a cryptographically optimized key generation scheme. This model uses metaheuristic optimization algorithms—such as the Modified Sooty Tern Optimization (MSFOA)—to generate high-entropy session keys that safeguard communications across all three layers. The keys are updated dynamically to protect against evolving threats, and the cryptographic process is lightweight to accommodate resource-constrained devices. By using an optimized cryptographic model, the TTEM framework balances strong security with minimal computational overhead. The communication process within TTEM follows a strict sequence of authenticated interactions. Each entity—Edge Device (ED), Fog Server (FS), Cloud Server (CS), and End User (EU)—undergoes registration with the CS before deployment. When a service request or data transmission is initiated, the EU or ED sends a login request to the FS, which validates the legitimacy of the request via the CS. Once mutual authentication is completed, secure session keys are exchanged to enable encrypted communication. This multi-step protocol ensures trust-based access and guards against eavesdropping or impersonation. In addition, peer-to-peer (P2P) capabilities at the edge layer allow for flexible and decentralized interactions among mobile devices, improving system resilience.

Trust Coordinator Election Process. It is suggested that each Fog Computing Domain (FCD) elects a Trust Coordinator (TC) using an election process based on three main aspects: uptime availability, history of consistent trustworthiness, and meeting Quality of Service (QoS) requirements. The TCs are chosen depending on the reliability score and the steady records of interaction with the nodes. MSFOA Variations: The Updated Sooty Tern Optimization Algorithm in TTEM has gone through the modifications of entropy feedback loops, load-aware particle seeding, and dynamic adjustments of inertia weight. These changes make sure that higher entropy session keys are generated with less overhead. The dynamism of the algorithm is changed based on the prediction of network congestion and network latencies, enhancing scalability and resilience.

To measure the benefits of offloading tasks across the triple-layered architecture, TTEM defines the relative computing efficiency of edge, fog, and cloud nodes. It considers the processing time and computational power of each type of node in comparison to a delegator (a coordinating edge node). When the computational efficiency of a worker node exceeds that of the delegator, task offloading results in significant speedup. Even when the efficiency is lower, combined parallel execution across multiple layers can enhance overall throughput. This reinforces the advantage of cooperative computing in a heterogeneous network, emphasizing TTEM's capability to manage complex workloads efficiently while maintaining service reliability.

4.1. Mathematical analysis of the proposed TTEM model

In the design of the Triple-layered Trust Evaluation Model (TTEM), mathematical modeling plays a vital role in quantifying trust, measuring user satisfaction, and evaluating performance efficiency across distributed cloud systems. By formulating trust and service satisfaction as quantifiable metrics, TTEM ensures objective evaluation of cloud service providers (CSPs), considering dynamic Quality of Service (QoS) attributes such as bandwidth, cost, memory availability, and reliability [21].

4.1.1. User satisfaction evaluation

User satisfaction is evaluated by comparing the provided Quality of Service (QoS) with the expected QoS values across four parameters: bandwidth, memory, cost, and reliability. The satisfaction score for a single service is computed as:

$$y = \frac{BW_p}{EBW_p} \cdot W_1 + \frac{Mem_p}{EMem_p} \cdot W_2 + \frac{Cost_p}{ECost_p} \cdot W_3 + \frac{Rel_p}{ERel_p} \cdot W_4 \quad (1)$$

Where:

- BW_p = Provided Bandwidth for service p
- EBW_p = Expected Bandwidth
- Mem_p, $EMem_p$ = Provided and Expected Memory
- $Cost_p$, $ECost_p$ = Actual and Expected Cost
- Rel_p, $ERel_p$ = Actual and Expected Reliability
- W_1, W_2, W_3, W_4 = Weights assigned by user preference for each QoS parameter

The overall satisfaction U_y for q services are computed as:

$$U_y = \frac{1}{q}\sum_{p=1}^{q} y_p \quad (2)$$

4.1.2. Trust evaluation via fog computing domains

To enable scalable trust evaluation, edge devices are grouped into Fog Computing Domains (FCDs). Each FCD elects a trust coordinator responsible for aggregating trust scores from its members. The trust score for a domain can be modeled as a function of the average user satisfaction across its nodes:

$$Trust_{FCD} = \frac{1}{n}\sum_{i=1}^{n} U_{y_i} \quad (3)$$

Where n is the number of users/devices in the domain.

4.1.3. Computation modeling across layers

Each computational node (edge, fog, cloud) is associated with a relative computing power κ and execution time τ for a given number of jobs m. Assuming the delegator is the reference edge node q_{e_1}The time taken by each type of node is modeled as:

$$\tau_{e_i} = \frac{\kappa_{e_i}}{\tau_{e_1}} \text{ for } 1 \le i \le X \quad (4)$$

$$\tau_{f_j} = \frac{\kappa_{f_j}}{\tau_{e_1}} \text{ for } 1 \le j \le Y \quad (5)$$

$$\tau_{c_l} = \frac{\kappa_{c_l}}{\tau_{e_1}} \text{ for } 1 \le l \le Z \quad (6)$$

Where:

- $\tau_{e_i}, \tau_{f_j}, \tau_{c_l}$ = Task completion times on edge, fog, and cloud nodes, respectively
- $\kappa_{e_i}, \kappa_{f_j}, \kappa_{c_l}$ = Relative computing power of each node

4.1.4. Theoretical speedup bound

Assuming ideal parallel execution with no communication overhead, the upper bound of speedup achievable using all participating nodes (edge, fog, and cloud) is given by:

$$S_b = 1 + \sum_{i=1}^{X} \frac{1}{\kappa_{e_i}} + \sum_{j=1}^{Y} \frac{1}{\kappa_{f_j}} + \sum_{l=1}^{Z} \frac{1}{\kappa_{c_l}} \quad (7)$$

This represents the maximum achievable acceleration when distributing tasks over all available computing resources in the TTEM model. A value of $\kappa < 1$ implies the worker node is faster than the delegator. Even for $\kappa > 1$Collaborative processing can still enhance throughput due to workload parallelism.

4.1.5. Trustworthiness index calculation

The trustworthiness index (TI) is calculated based on the average of the transparency score.TS) and performance score (PS) of each algorithm:

$$TI = \frac{TS+PS}{2} \quad (8)$$

This metric is used to compare various algorithms and validate the efficiency of TTEM against existing methods such as GA, CSA, and MSFOA.

This mathematical analysis section has established a foundational understanding of the TTEM model's quantitative structure. The proposed framework applies adaptive trust scoring, session key optimization, and theoretical speedup modeling to achieve performance efficiency and secure decision-making in heterogeneous cloud systems. These mathematical insights not only validate TTEM's structural integrity but also ensure that the proposed model remains responsive to user preferences, network dynamics, and resource capabilities. By integrating trust computation with latency-aware optimization, TTEM proves to be a highly applicable model for real-world applications like healthcare monitoring and smart infrastructure management

5. Results analysis

This section presents the simulating investigation, which employs a trust module and a new optimized scheme to protect the DPP of CSP. The trust model assesses the trustworthiness of CSPs using criteria such as reputation, compliance, and user input, whilst the new encryption model ensures data security. To optimize trust and key strength factors, the TTEM algorithm is used. Dataset resources for privacy preservation in the cloud with machine learning have been collected from [22].

It presents a trust model, which is used to create trust scores for CSPs, i.e., used to generate trust scores throughout ten iterations, including two SP and 3 devices (Figure 4). The trust model, which was tested across ten rounds, is useful to assess CSPs in industries that prioritize security like financial dealings, healthcare schemes, and so on. In every iteration, the trust modelling analyses historical data and user feedback on their interactions with various CSPs.

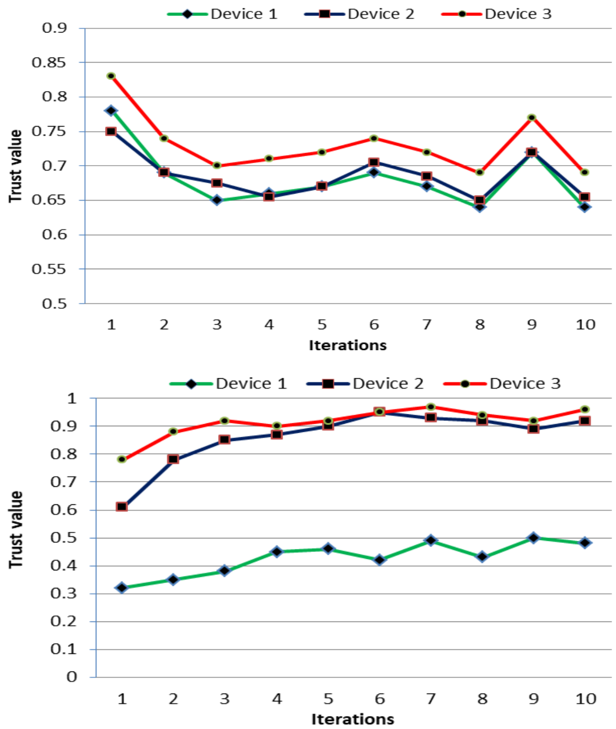

Fig. 4: Trust Models of Two Cloud Service Providers: (A) Service Provider 1 and (B) Service Provider 2.

The TTEM responds dynamically to shifting CSP performance, thus being suitable for dynamic service contexts. The new encryption paradigm, which protects data secrecy, is especially useful for services that handle sensitive information. These data elements are evaluated and aggregated to generate a trust score for every CSP. The TTEM model gives higher trust scores to CSPs who have shown consistent reliability, conformance to security standards, and favourable customer feedback. CSPs with a track record of security breaches, noncompliance, or poor user feedback, on the other hand, have lower trust rankings. The TTEM model's iterative structure enables it to adjust and update trust scores in response to changing CSP performance and evolving user feedback. The trust scores given by the TTEM model afford useful information about the trustworthiness and reliability of CSPs. It will be utilised to make decisions when selecting CSPs. The highest trust scores imply the greatest confidence level to protect privacy, secure data, and provide dependable CS. The use of the TTEM model to generate trust ratings for CSPs over numerous iterations provides a strong and dependable method for assessing CSP trustworthiness. It adds to the entire TTEM mechanism by adding the trust feature as a crucial component in CSP.

Table 1 compares three algorithms (GA, GA-CSA, and MSFOA) and a projected model (a new approach combining MSFOA and layered algorithms) based on their performance in terms of computing time, utilization of resources, trustworthy index, performance, and transparency rates (scores), demonstrating its dependability for security-centric services. The Trustworthy Index (TI) is assessed by averaging the Performance and Transparency Scores as per equation 3.

$$\text{TI} = (\text{Performance} + \text{Transparency}) / 2 \quad (3)$$

It assesses the overall trustworthiness rating for every module in the trust-based confidentiality protection system.

Table 1: Performance Assessment

Algorithm	Computational time	Trustworthiness Index	Resource utilization	Transparency score	Performance score
GA	0.461	0.867	0.752	0.912	0.839
CSA	0.45	0.879	0.88	0.84	0.90
GA-CSA	0.467	0.887	0.905	0.884	0.914
MSFOA	0.441	0.903	0.937	0.926	0.933
TTEM	0.425	0.91	0.95	0.94	0.941

Depending on the tabulated values, the TTEM system has a computing time of 0.425, utilization of resource of 0.95, performance rate of 0.941, transparency rate of 0.94, and trustworthy index of 0.91.

The newly proposed TTEM-based multi-cloud solution for storage and security enhancement has been instigated in the MATLAB / Simulink environment. A good foundation for the rapid development of numerous technologies yields absolute outcomes, enabling multi-cloud storage concept using new DPP approaches. In addition, four different cloud storage providers are also used in this strategy (Google Drive, MediaFire, PCloud, and MEGA as the major datasets) to carry out the simulating setup. The innovative TTEM method considers two factors for multi-cloud optimization: upload time and access latency. There will occasionally be variances in the properties of original CSP. Table 2 shows the TTEM optimization technique as the first step in minimizing access latency time (Figure 5). This is obtained for the four separate data sets stated previously. The upload time associated with every CSP is subsequently taken into consideration. Table 3 shows that the sizes of 25, 50, 75, and 100 MB are optimized for four clouds. As a result, the data were separated into four groups based on the total quantity of CSP utilized throughout the experiment.

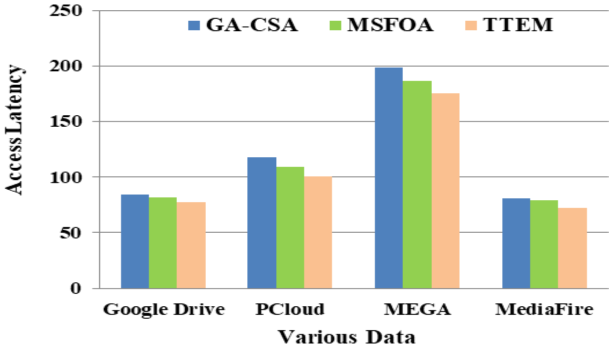

Fig. 5: Comparison of Access Latency.

Table 2: TTEM with Access Latency

Methods	Data			
	Google Drive	PCloud	MEGA	MediaFire
GA-CSA	84	118	199	81
MSFOA	82	109	187	79
TTEM	77	101	175	72

Table 3: DPTPTS with Upload Time

Methods	File size (MB)			
	25	50	75	100
GA-CSA	94	81	188	119
MSFOA	89	76	164	102
TTEM	76	64	144	98

When tested on the dataset, the proposed TTEM technique outperforms standard models. Regarding the analyses of multi-cloud security and storage, the suggested TTEM method provides a significant improvement. This technology is particularly well-suited for smart city applications, such as urban disaster notifications, by enabling real-time data collection and response. In the context of developing a flood decision support system, fog nodes gather real-time data on urban water levels and issue early warnings and alerts when flood risks are detected. Additionally, it has significant applications in healthcare. By monitoring and analyzing pulse data between an edge device linked to the user's smartphone and a cloud server, the system can determine if the user has fallen or is experiencing other emergencies at home, thereby facilitating prompt medical assistance. According to human needs, this concept will be suitable for all smart application systems. To mitigate trust bias, the TTEM framework will be extended using anomaly detection algorithms like Isolation Forests and unsupervised clustering (e.g., DBSCAN) to identify abnormal trust behavior. Reputation decay mechanisms will also be introduced, wherein trust scores degrade over time in the absence of recent interactions.

6. Conclusion

In this research, a novel Triple-layered Trust Evaluation Model (TTEM) was proposed to address the critical challenges of trust management, data security, and performance optimization in dynamic cloud service environments. By leveraging a hierarchical architecture composed of edge, fog, and cloud layers, the model ensures low-latency communication, efficient task offloading, and scalable trust computation across distributed nodes. The integration of optimized cryptographic key generation mechanisms enhances data confidentiality and access control, making TTEM particularly suitable for privacy-sensitive applications such as healthcare, smart infrastructure, and industrial IoT. The TTEM model dynamically evaluates trust by considering user-defined Quality of Service (QoS) parameters such as bandwidth, memory, cost, and reliability. Trust scores are computed and updated in real-time using fog-based coordinators, ensuring that service provider evaluations remain adaptive and accurate. Furthermore, the use of mathematical modeling and simulation demonstrates the effectiveness of TTEM in achieving significant improvements in resource utilization, task execution time, and trustworthiness compared to existing methods such as GA, CSA, and MSFOA. The simulation results confirm that TTEM not only meets security and performance goals but also enhances service transparency and user satisfaction. However, the study also acknowledges that trust-based systems are inherently vulnerable to bias and manipulation. As part of future work, further investigation will focus on mitigating trust bias, detecting malicious nodes, and integrating context-aware trust mechanisms to further enhance resilience. Additionally, deployment of TTEM in real-world multi-cloud environments and benchmarking with larger datasets will be explored to validate its scalability and robustness. Overall, TTEM presents a comprehensive and effective framework for secure, trustworthy, and performance-optimized data storage management in dynamic multi-cloud systems.

References

[1] Tricomi, G., Merlino, G., Panarello, A. and Puliafito, A., 2020. Optimal selection techniques for Cloud service providers. *IEEE Access*, *8*, pp.203591-203618. https://doi.org/10.1109/ACCESS.2020.3035816.

[2] Khan, M.A., Khan, S.M. and Subramaniam, S.K., 2023. Secured Dynamic Request Scheduling and Optimal CSP Selection for Analyzing Cloud Service Performance Using Intelligent Approaches. *IEEE Access*, *11*, pp.140914-140933. https://doi.org/10.1109/ACCESS.2023.3339378.

[3] Angel, N.A., Ravindran, D., Vincent, P.D.R., Srinivasan, K. and Hu, Y.C., 2021. Recent advances in evolving computing paradigms: Cloud, edge, and fog technologies. *Sensors*, *22*(1), p.196. https://doi.org/10.3390/s22010196.

[4] Kuchuk, H. and Malokhvii, E., 2024. Integration of IoT with cloud, fog, and edge computing: a review. *Advanced Information Systems*, *8*(2), pp.65-78. https://doi.org/10.20998/2522-9052.2024.2.08.

[5] Naouri, A., Nouri, N.A., Khelloufi, A., Sada, A.B., Ning, H. and Dhelim, S., 2024. Efficient fog node placement using nature-inspired metaheuristic for IoT applications. *Cluster Computing*, *27*(6), pp.8225-8241. https://doi.org/10.1007/s10586-024-04409-3.

[6] Kumar, T., Sharma, P., Cheng, X., Lalar, S., Kumar, S. and Bansal, S., 2025. Enhanced Triple Layered Approach for Mitigating Security Risks in Cloud. *Computers, Materials and Continua*, *83*(1), pp.719-738. https://doi.org/10.32604/cmc.2025.060836.

[7] Jangjou, M. and Sohrabi, M.K., 2022. A comprehensive survey on security challenges in different network layers in cloud computing. Archives of Computational Methods in Engineering, 29(6), pp.3587-3608. https://doi.org/10.1007/s11831-022-09708-9.

[8] Abba Ari, A.A., Ngangmo, O.K., Titouna, C., Thiare, O., Mohamadou, A. and Gueroui, A.M., 2024. Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges. *Applied Computing and Informatics*, *20*(1/2), pp.119-141. https://doi.org/10.1016/j.aci.2019.11.005.

[9] Raja, V., 2024. Exploring challenges and solutions in cloud computing: A review of data security and privacy concerns. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *4*(1), pp.121-144. https://doi.org/10.60087/jaigs.v4i1.86.

[10] John, J. and John Singh, K., 2024. Trust value evaluation of cloud service providers using fuzzy inference based analytical process. *Scientific Reports*, *14*(1), p.18028. https://doi.org/10.1038/s41598-024-69134-8.

[11] Balcão-Filho, A., Ruiz, N., de Franco Rosa, F., Bonacin, R. and Jino, M., 2021. Applying a consumer-centric framework for trust assessment of cloud computing service providers. *IEEE Transactions on Services Computing*, *16*(1), pp.95-107. https://doi.org/10.1109/TSC.2021.3134125.

[12] Li, Y., Cao, Y., Zhuang, Y., Li, J., Du, G. and Chen, J., 2024. Blockchain-enabled trust management with location privacy preservation in vehicular ad hoc networks. *IEEE Internet of Things Journal*, *11*(14), pp.24659-24671. https://doi.org/10.1109/JIOT.2024.3350694.

[13] Chen, Y.C., Yang, J.K., Yen, H.C. and Lin, P.W., 2024. Dual-Cloud Multi-Secret Sharing Architecture for Privacy Preserving Persistent Computation. *IEEE Transactions on Information Forensics and Security*. https://doi.org/10.1109/TIFS.2024.3436662.

[14] Sugitha, G. and S, A.L., 2024. A multi-objective privacy preservation model for cloud security using hunter prey optimization algorithm. *Peer-to-Peer Networking and Applications*, *17*(2), pp.911-923. https://doi.org/10.1007/s12083-023-01591-w.

[15] Firouzi, F., Farahani, B. and Marinšek, A., 2022. The convergence and interplay of edge, fog, and cloud in the AI-driven Internet of Things (IoT). *Information Systems*, *107*, p.101840. https://doi.org/10.1016/j.is.2021.101840.

[16] Shirazi, S.N., Gouglidis, A., Farshad, A. and Hutchison, D., 2017. The extended cloud: Review and analysis of mobile edge computing and fog from a security and resilience perspective. *IEEE Journal on Selected Areas in Communications*, *35*(11), pp.2586-2595. https://doi.org/10.1109/JSAC.2017.2760478.

[17] Wang, S.; Zhang, X.; Zhang, Y.; Wang, L.; Yang, J.; Wang, W. A survey on mobile edge networks: Convergence of computing, caching and communications. IEEE Access 2017, 5, 6757–6779. https://doi.org/10.1109/ACCESS.2017.2685434.

[18] Ren, J.; Yu, G.; He, Y.; Li, G.Y. Collaborative cloud and edge computing for latency minimization. IEEE Trans. Veh. Technol. 2019, 68, 5031–5044. https://doi.org/10.1109/TVT.2019.2904244.

[19] Shi, W.; Cao, J.; Zhang, Q.; Li, Y.; Xu, L. Edge computing: Vision and challenges. IEEE Internet Things J. 2016, 3, 637–646. https://doi.org/10.1109/JIOT.2016.2579198.

[20] Cruz, P.; Achir, N.; Viana, A.C. On the Edge of the Deployment: A Survey on Multi- Access Edge Computing. ACM Comput. Surv. (CSUR) 2022, 55, 1–34. https://doi.org/10.1145/3529758.

[21] Deshpande, S. and Ingle, R., 2018. Evidence based trust estimation model for cloud computing services. *Int. J. Netw. Secur.*, *20*(2), pp.291-303.

[22] https://www.kaggle.com/code/naifaganadily/privacypreserving-machine-learning.