International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 5, 2025
https://theaspd.com/index.php

Utilization Of Compact Three-Layered Model For Privacy Preserving Of Storage Data In Cloud Computing

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, spbalamurugan@rediffmail.com

Abstract
Cloud services are cloud computing (CC) applications and resources that are distributed on the Internet or a CC platform, allowing users to access at any time. But the user may face some issues while analyzing and selecting cloud service providers (CSP). As a result, it is critical to research and develop an objective and effective trust model in order to increase user interaction and satisfaction success rates. The growing importance of privacy preservation along with trust in CC atmospheres protects sensitive data and sustains user confidence in the privacy concerns. However, the dependability of such systems is regularly impacted by issues with trust assessment security vulnerabilities, and resource allocation. This research proposes a novel trust model, and key strengthening with privacy-preserving method called data privacy and trust preserving triple-layered storage model (DPTPTS). It enables efficient real-time data handling, supports scalable infrastructure, and ensures better use of available resources. A trust-based framework assists users in selecting suitable cloud service providers (CSPs) by considering important factors such as data storage and processing requirements. One of the main advantages lies in evaluating the strength of encryption keys used to protect confidential information. This helps in defending against unauthorized access and security breaches. By enhancing key strength, users can maintain privacy and ensure data protection in cloud environments. Applying this optimized key management approach across multiple cloud platforms results in improved performance and stronger data security.
Keywords: *Multi-cloud, three-layered module, key optimizer, trust-based security, privacy protection.*

1. INTRODUCTION

Privacy preservation has emerged as a key concern in the age of CC because to the massive volume of sensitive data processed and stored on the cloud. Launching trust among CSP and cloud users is an important part of controlling privacy issues in cloud systems [1]. Users rely on CSP for handling those data by means of the utmost confidentiality and privacy; thus, trust is essential when evaluating the dependability, security and integrity of CS. Confidence- based privacy preserving solutions aim to enhance data security and promote trust among cloud users and CSP [2].

Conversely, the numerous benefits of CC are coupled by considerable risks, particularly with data security. With a growing variety of documents, communications, records and applications that rely on processing and storage by remote servers, usually operated by irrelevant parties, the integrity and confidentiality of processed and stored data becomes gradually significant [3]. It necessitates protecting people and the information stored in its structures to prevent undesirable usage, access, or breaches. It requires managing the risks that come with sharing, various tenants, and resource exchange among diverse networks. To this purpose, challenges of privacy have been aggravated by modern rules, which mandate high-standard data protection measures.

On the other hand, successful implementation and management of these frameworks pose numerous significant obstacles. Trust is essential for enabling secure interactions between distributed IoT devices and cloud-edge systems, particularly in cases where data is exchanged across disparate devices and networks. Security measures are critical for protecting sensitive data and infrastructure from illegal access, cyber-attacks, and system failures. Simultaneously, resource management is critical for balancing computing workloads, optimizing energy usage, and ensuring QoS (Quality of Service) by offering, low latency, and mobility [4]. The combined use of cloud-edge computing necessitates robust systems for handling massive volumes of data, ensuring reliable connectivity, and maintaining system integrity under changing conditions. The customers must navigate the diversity and complexity of QoS. Furthermore, the demand for energy-efficient solutions grows in industrial applications wherever sustainability and cost-

effectiveness are top objectives [5].

approaches have emerged as effective mechanisms that enable users to assess the reliability of Cloud computing (CC) has transformed the way data and services are delivered by offering scalable, on-demand resources over the internet. While this paradigm enables cost-efficient storage and processing, it simultaneously raises concerns over data security, user trust, and privacy preservation. As users increasingly rely on Cloud Service Providers (CSPs) to manage sensitive information, the need for robust security frameworks has become paramount. Traditional privacy-preserving methods focus primarily on encryption and access control; however, they often fall short in addressing insider threats and dynamic trust variations among CSPs [6].

To overcome these challenges, trust-based computation and resource allocation frameworks have gained attention from the existing method [7] proposed a trust-based offloading framework in mobile cloud-edge computing networks, highlighting the role of trust in securing data transmission and offloading decisions. Their work emphasized that without proper trust evaluation, even advanced offloading strategies could lead to compromised data confidentiality. Similarly, from the existing method [8] introduced a trust-security-resource optimization (TSRO) framework designed for cloud-edge-IoT collaboration in industrial applications. Their findings show that integrating trust metrics into resource allocation not only improves security but also enhances system efficiency and user satisfaction.

Building on these developments, this study proposes a comprehensive Data Privacy and Trust Preserving Triple-Layered Storage (DPTPTS) model. It addresses existing gaps by combining multi-layered storage architecture with optimized trust evaluation, secure data partitioning, and entropy-based key generation. By incorporating contextual intelligence (CI) for dynamic data distribution and leveraging erasure coding for fault tolerance, the DPTPTS model aims to offer a scalable, secure, and privacy-aware solution for modern cloud environments.

- To suggest new data privacy and trust preservation triple-layered storage model (DPTPTS) for effective trust and secured-based data storage mechanism.
- To provide the best optimization progress in generating strong key for highly protected data.
- To improve QoS, the model is designed as a joint optimization problem, with the goal of maximizing trust while minimizing communication delay.
- To evaluate trust as a quantitative property and the trust levels of several CSPs are compared using the proposed quality attributes. The quality attribute values are estimated using a simulated environment and a set of metrics.

The remaining sections are provided one-by-one as literature reviews, overview of the methodology, proposed DPTPTS model, simulation with outcomes and ends with the conclusion part.

2. LITERATURE SURVEY

Cloud computing (CC) has revolutionized how organizations and individuals operate by offering unmatched scalability, flexibility, and cost-efficiency. To fully leverage these advantages, many enterprises are increasingly migrating their data and applications to cloud environments. However, with the growing adoption of cloud services, concerns around data privacy have also intensified. Recent advancements in cloud computing have underscored the importance of developing intelligent privacy-preserving mechanisms to protect data while enabling efficient and scalable storage solutions. Numerous researchers have contributed to this area by integrating hybrid optimization, trust assessment, and secure storage frameworks.

Saini et al. (2024) [9] proposed a hybrid optimization and machine learning framework aimed at enhancing both trust and security in cloud networks. Their model demonstrated that combining metaheuristic algorithms with learning-based adaptations significantly improves the reliability of trust scoring mechanisms in dynamic cloud environments. This approach aligns with the motivation of the DPTPTS model, which integrates trust evaluations into multi-cloud storage decisions. Expanding on this, Saini, Singh, and Rohil (2023) [10] developed a hybrid metaheuristic optimization algorithm for trust-aware privacy preservation. Their work tackled the challenge of balancing privacy constraints with computational efficiency in distributed cloud environments. The proposed hybrid strategy proved effective in managing sensitive data, inspiring the integration of optimization-based key generation and

trust metrics in the present study.

Further progress was made by Dhamdhere et al. (2025) [11], who introduced a deep learning-assisted sanitization and restoration framework for cloud data. Their Deep Maxout model facilitated more accurate detection and reconstruction of sensitive information, allowing improved control over privacy during cloud transactions. This highlights the need for intelligent encoding and restoration capabilities, which are incorporated into the DPTPTS model through its MSFOA-assisted encoding and decoding processes. Finally, Chen and Huang (2025) [12] presented a privacy-preserving federated learning model specifically designed for airline upgrade optimization. Their work revealed the criticality of maintaining data confidentiality in collaborative learning environments and demonstrated how privacy-focused strategies can be adapted to real-time applications. This insight reinforces the necessity of scalable, secure frameworks like DPTPTS, which aim to protect sensitive data in distributed systems without sacrificing performance or usability.

Collectively, these studies emphasize the growing shift toward hybrid, trust-based, and learning-supported cloud security architectures. The DPTPTS model builds upon these foundational works by offering a unified solution that integrates trust scoring, secure data partitioning, and optimization-driven key generation within a three-layered multi-cloud environment.

In addition to trust and optimization strategies, recent studies have also emphasized the significance of intelligent algorithms and enhanced data sanitization techniques in preserving privacy within cloud environments. Yu et al. (2025) [13] introduced an improved Red-Tailed Eagle Algorithm, inspired by biomechanics, to optimize parameter identification in complex systems such as photovoltaic cells. Though primarily applied to renewable energy systems, the algorithm's strength in solving global optimization problems highlights its potential relevance to privacy-preserving applications. Their approach underlines how bio-inspired methods can offer robust solutions to parameter tuning and trust-based evaluation, which informs the optimization logic within the DPTPTS framework.

Shivashankar and Mary (2021) [14] proposed a modified Rider Optimization Algorithm for data sanitization and restoration, designed to enhance privacy protection while maintaining data integrity. Their model included optimal transformation strategies to obscure sensitive information effectively without excessive data distortion. This concept directly supports the sanitization and restoration mechanism of the proposed DPTPTS model, which also aims to balance privacy with performance by using a multi-objective optimization approach integrated with erasure coding. Together, these contributions reinforce the growing reliance on intelligent, nature-inspired algorithms for handling privacy and trust challenges in multi-cloud storage systems. The DPTPTS model builds upon these ideas by integrating trust-aware optimization, strong key generation, and decentralized data storage in a secure, triple-layered architecture.

3. OVERVIEW OF METHODOLOGY

Conventional encryption-based privacy methods often fail to defend against insider threats within cloud storage systems. To overcome this, the proposed DPTPTS model introduces a triple-layered architecture built on cloud computing principles. It leverages optimized erasure coding and contextual intelligence (CI) to partition and distribute data securely across three layers: local (edge), fog, and cloud servers. During the upload process, data is first encoded using a modified hash algorithm. This algorithm segments the data into blocks, with a small portion (approximately 1%) stored locally, and the remainder distributed across fog and cloud layers. Fog nodes, characterized by limited storage and processing capacity, serve as intermediaries for real-time or delay-sensitive data processing. CI dynamically determines the optimal ratio of data distribution between the three layers.

To enhance redundancy and fault tolerance, erasure coding is applied twice—once during initial segmentation and again before cloud upload. This ensures that partial data cannot reconstruct the original content, enhancing privacy. Around 6% of encoded blocks are retained in the fog layer, while approximately 94% are uploaded to the cloud. The cloud layer then redistributes the data across multiple cloud service providers. In the storage process, erasure coding reduces bandwidth usage and enhances reliability by sending one block of data to each of the selected cloud providers. The fog layer handles latency-sensitive processing, whereas less critical data is routed to aggregate nodes for deeper analysis and

later sent to the cloud for long-term storage. Time-insensitive data is retained in the cloud and can be analyzed or retrieved as needed. By combining trust-based storage allocation, erasure coding, and CI-driven decisions, the DPTPTS framework ensures secure, scalable, and efficient data management across multi-cloud infrastructures.

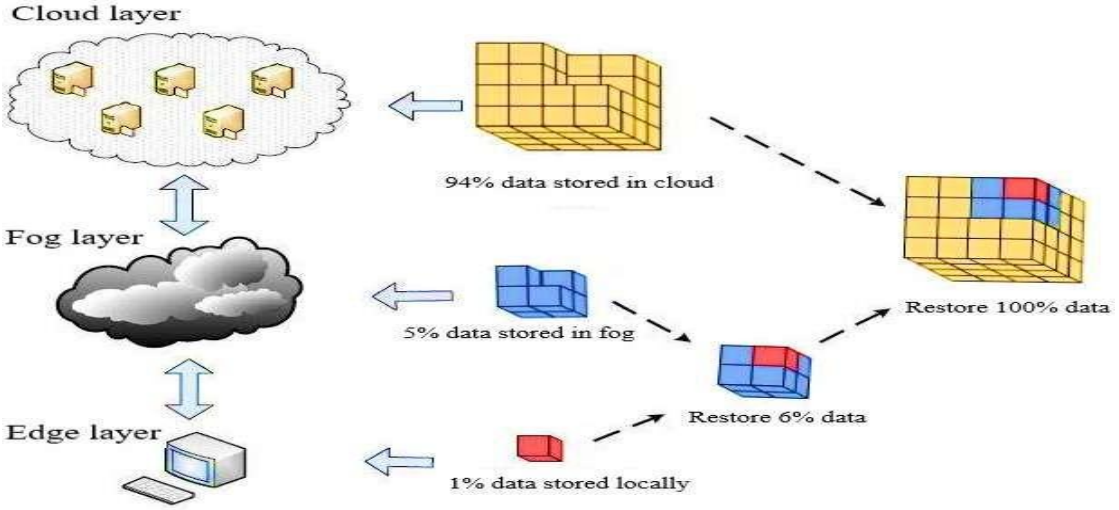


Figure 1 Cloud managing system

Downloading process: During the file retrieval process, the user initiates a request to the cloud server for downloading the desired data. In response, the cloud server aggregates the necessary data segments from various distributed storage points and transmits approximately 94% of the total data to the corresponding fog layer. Once the fog server receives this data, it combines it with locally stored encoded segments—accounting for around 6%—to reconstruct nearly 98% of the complete file. Subsequently, about 11% of the processed data is forwarded from the fog server to the user. This sequential recovery and reassembly process continues until the user obtains the full dataset. The layered retrieval mechanism ensures secure and efficient data delivery while minimizing the dependency on any single storage node [18].

4. Proposed Dptpts Model

A unique TS storage model with a CC mechanism has been suggested. This architecture takes advantage of the benefits of cloud storage whereas protecting data privacy. In the new concept, the erasure coding with MO-DPPT and MSFOA technique for effective trust-based multi-cloud storage is utilized by splitting them as TS structure as depicted in Figure 2

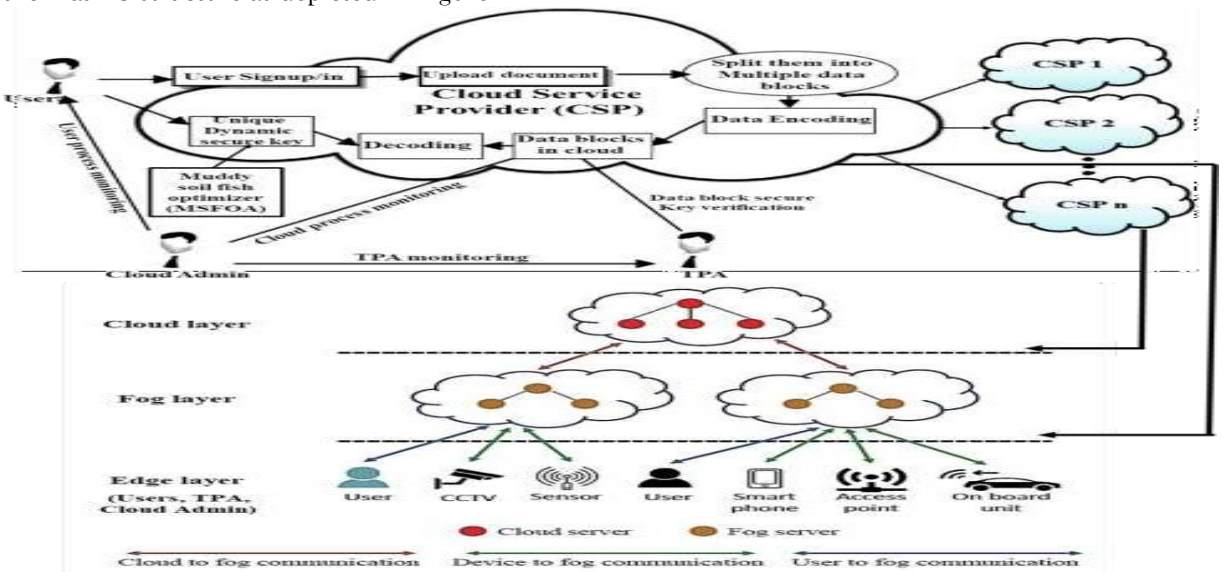


Figure 2: Proposed triple-layered structure in multi-cloud storage environment

The submitted MSFOA-based MO-DPPT system model includes two critical processes: data sanitization and data restoration. Data sanitization is a strategy for concealing sensitive data in a cloud setting. The

optimal key generation method is standardized by considering the multi-objective function, which includes some characteristics or simulation metrics. A sanitization and restoration model that considers objective functions such as information preservation rate (PR), hiding failure rate (HR), false rule generation rate (FR), and degree of modification (DM) is recommended for better privacy data preservation. During sanitization and restoration, an ideal key is generated using a hybrid model known as the Genetic Algorithm with Crow Search Algorithm [19] (GA-CSA). Furthermore, the authorised user within the receiving end successfully restores the sensitive data. This strategy seeks to prevent leaks to unauthorized locations. The proposed sanitization process is then carried out using a meta-heuristic algorithm known as MSFOA, which is optimized for key generation. It is validated by third-party authentication (TPA). The administrator acts as an intermediary for the user and the TPA. Administrator checks monitor both the user and the TPA wherever the TPA checks the optimized keys as a result of the user's activity. The administrator monitors the whole of CS procedure. The highly secured erasure encoding, decoding, key optimizations in multiple CS procedures are followed similarly as in the approach [20].

The suggested MSFOA may efficiently execute data sanitization and restoration for cloud data security by leveraging this multi-objective function. Similarly, the process of extracting sensitive data using the unique key employed in the data cleansing process is referred to as data restoration. To address global optimization problems, these algorithms provide the best answers. Because of their adaptability, these population-based algorithms may efficiently address multi- objective problems and produce predicted results. Furthermore, these algorithms will be free of constraints in order to meet the goal function while also accounting for system model limits. Most importantly, the proposed MSFOA algorithm attempts to control the cost when compared to a centralized methodology by combining distributed notions with efficient calculation. The convergence of cloud, fog, and edge technologies called TLS model has altered industrial operations, and these layers are also briefly described here.

User/edge layer: The model considers multiple factors—such as the reputation of cloud service providers (CSPs), adherence to regulatory standards, and customer feedback—to evaluate their trustworthiness. This trust framework assists users in selecting suitable CSPs for data storage and processing based on these key criteria. During the trust evaluation phase, relevant trust metrics are gathered and synthesized to produce a comprehensive assessment of each CSP. Following this, the key strength evaluation phase identifies the optimal key size, generates cryptographic keys, and verifies their robustness. Together, these two dimensions—trust assessment and cryptographic strength—guide secure decision-making. The proposed technique enhances data protection by segmenting data into discrete units using a novel hash code algorithm and distributing these segments across local devices, fog nodes, and cloud storage. This approach not only strengthens data privacy but also improves storage efficiency. Contextual Intelligence (CI) plays a crucial role in determining the optimal distribution of data among these layers, ensuring both security and load balancing in the overall storage framework [21].

Fog layer: This layer is made up of several fog nodes placed at the network's edge. Fog nodes often include routers, gateways, switches, access points, base stations, and dedicated fog servers. Fog nodes can be deployed among terminal devices and the cloud, including mobile and static devices. They can process, transmit, and store sensing data, enabling real-time analysis and delay-sensitive applications within the fog layer. Fog nodes connect to cloud data centers and IP core networks, allowing for enhanced processing and storage capabilities.

Cloud layer: The cloud layer consists of high-performance servers and storage devices that enable smart application services. This layer's compute and storage capabilities enable extensive analysis and storing of massive amounts of data. Fog computing differs from standard CC by not relying solely on the cloud for computation and storage. The demand load concept suggests using control mechanisms to optimize cloud resource consumption.

Secured Cloud storage using DPTPTS

The DPTPTS model employs a three-tiered storage architecture comprising the user (local), fog, and cloud layers to enhance data security and privacy in cloud environments. In this design, data is segmented into three encoded portions using hash-based techniques and distributed across the layers—local, fog, and cloud—such that each segment is incomplete on its own. This prevents any single layer, including the

cloud service provider (CSP), from reconstructing the original data independently, thereby mitigating insider threats. The model incorporates erasure coding, where data is divided into k parts and extended with m redundant blocks, ensuring that the full dataset can only be reconstructed if at least k blocks are available. This mechanism enhances both privacy and fault tolerance. Additionally, the fog layer utilizes contextual intelligence (CI) to determine optimal values for k and m, adapting to the computational capabilities of each node. The data owner maintains control over file uploads, applies message authentication codes (MACs), and can monitor access and storage activity across layers. Notably, the fog layer plays a crucial role in full data recovery, as some portions are intentionally retained there to prevent complete access through the cloud layer alone. This layered strategy effectively secures user data against unauthorized access and supports efficient, privacy-preserving cloud storage management [22].

Once the owner uploads a file to the cloud, the file details can be accessed there. Cloud layer may also assess user request specifics and download file history. In the user/edge layer, user functionalities will be designed. The user can examine the available files and issue a request to access them. Upon receiving the well-optimized and secured key from the data owner, the user can completely download the file.

Mathematical Analysis of Secure Multi-Cloud Task Scheduling

The suggested Data Privacy and Trust Preserving Triple-Layered Storage (DPTPTS) paradigm is mathematically supported here. This research defines and quantifies the fundamental components of safe, efficient, and reliable data processing across several cloud tiers. It includes formal modeling for assessing Cloud Service Providers (CSPs) trustworthiness, measuring cryptographic key strength, segmenting and distributing data using erasure coding and hashing, and optimizing system performance using multi-objective criteria. CSP trust ratings are calculated using dynamic criteria such service dependability, past user interactions, and indirect recommendations. Strong encryption is ensured via entropy-based key strength analysis. Data is distributed among user, fog, and cloud levels in precise proportions to protect privacy and system efficiency. This mathematical research verifies and logically supports the DPTPTS model's privacy protection and trust-based decision-making in cloud contexts.

Objective Functions

The optimization problem aims to balance multiple objectives:

{1. Minimize Total Cost}

$$Z_1 = \sum_{i=1}^{n} \sum_{j=1}^{m} x_{ij} \cdot \text{Cost}(t_i, c_j) \tag{1}$$

{2. Minimize Execution Time}

$$Z_2 = \sum_{i=1}^{n} \sum_{j=1}^{m} x_{ij} \cdot \text{Time}(t_i, c_j) \tag{2}$$

{3. Maximize Availability}

$$Z_3 = \sum_{i=1}^{n} \sum_{j=1}^{m} x_{ij} \cdot A(c_j) \tag{3}$$

{4. Maximize Data Security}

$$Z_4 = \sum_{i=1}^{n} \sum_{j=1}^{m} x_{ij} \cdot S(t_i, c_j) \tag{4}$$

Constraints

{1. Task Assignment Constraint}

Each task must be assigned to exactly one cloud provider:

$$\sum_{j=1}^{m} x_{ij} = 1, \forall i = 1, \dots, n \tag{5}$$

{2. Cloud Resource Capacity Constraint}

The total demand from all assigned tasks should not exceed a cloud's capacity:

$$\sum_{i=1}^{n} x_{ij} \cdot R(t_i) \leq Cap(c_j), \forall j = 1, \ldots, m \quad (6)$$

{3. Task Dependency Constraint (for PDTs)}

A task must start only after its predecessor has completed:

$$Start(t_j) \geq Finish(t_i), \text{ if } t_i \rightarrow t_j \quad (7)$$

Erasure Coding Analysis

Let (n, k) be erasure coding parameters:

{4. Storage Overhead}

$$Overhead = \frac{n}{k} \quad (8)$$

{5. Availability Probability}

If each cloud has availability p, and data is retrievable from any k of n clouds:

$$P_{avail} = \sum_{i=k}^{n} \binom{n}{i} \cdot p^i \cdot (1-p)^{n-i} \quad (9)$$

Final Multi-Objective Optimization

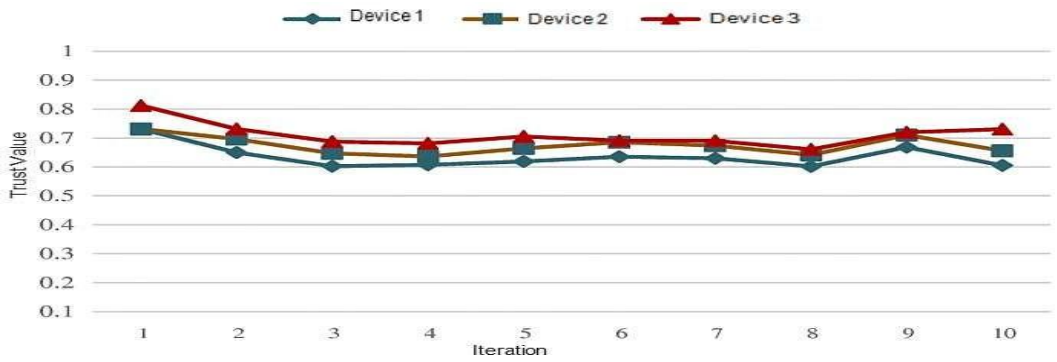
$$\text{Optimize } \{Z_1, Z_2, -Z_3, -Z_4\} \text{ subject to constraints (5)–(7)} \quad (10)$$

The mathematical study shows that the DPTPTS model manages and secures sensitive data in multi-cloud storage systems. Trust assessment equations employ service-level data and indirect feedback to evaluate CSP dependability. Shannon entropy calculations verify cryptographic key strength, preventing attacks. Data is securely divided and distributed across edge, fog, and cloud levels using erasure coding and hash-based methods. Optimizers balance hidden failure rate, information preservation, false rule creation, and data modification. Different algorithmic techniques are evaluated and compared using a performance-based trustworthiness measure. These mathematical formulations provide the DPTPTS model a solid theoretical foundation and show its potential to achieve security, efficiency, and privacy requirements in real-time cloud computing settings.

5. RESULTS ANALYSES

This section presents the simulating investigation, which employ a trust module and 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 DPTPTS algorithm is used. Dataset resources for privacy preservation in the cloud with machine learning have been collected from the following sites: https://www.kaggle.com/code/naifaganadily/privacypreserving-machine-learning.

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 three SP and 3 devices (Figure 3). 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.



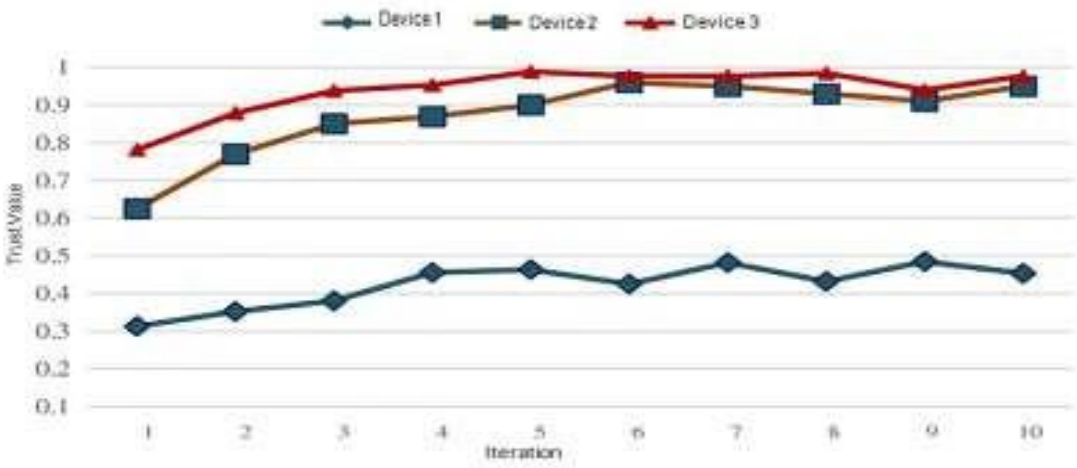


Figure 3. Trust Model

The DPTPTS 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 DPTPTS 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 DPTPTS 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 DPTPTS 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 DPTPTS 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 DPTPTS mechanism by adding the trust feature as a crucial component in CSP.

Table 2 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 resource, 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.

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

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	0.46	0.868	0.751	0.902	0.837
GA-CSA	0.531	0.886	0.878	0.839	0.912
MSFOA	0.567	0.89	0.91	0.89	0.911
DPTPTS	0.491	0.908	0.942	0.934	0.937

Depending on the tabulated values, the DPTPTS system has the computing time of 0.49, utilization of resource of 0.942, performance rate of 0.937, transparency rate of 0.934, and trustworthy index of 0. 908. The newly proposed DPTPTS-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 DPTPTS 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 DPTPTS optimization technique as the first step in minimizing access latency time. 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.

Table 2: DPTPTS with Access Latency

Methods	Data			
	Google Drive	PCloud	MEGA	MediaFire
MSFOA	84	118	199	81
DPTPTS method	82	109	187	79

Table 3: DPTPTS with upload time

Methods	File size (MB)			
	25	50	75	100
MSFOA	94	81	188	119
DPTPTS method	89	76	164	102

When tested on the dataset, the proposed DPTPTS technique outperforms standard models. Regarding the analyses of multi-cloud security and storage, the suggested DPTPTS method provides a significant improvement.

6. CONCLUSION

This research introduced a novel Data Privacy and Trust Preserving Triple-Layered Storage (DPTPTS) model to address the growing concerns of data security, trust management, and resource optimization in cloud computing environments. By integrating user/edge, fog, and cloud layers within a unified architecture, the model ensures secure and efficient data handling. It employs optimized cryptographic key generation, trust-based CSP evaluation, and erasure coding to segment and distribute data intelligently, thereby preserving privacy and enhancing system reliability. Simulation results and mathematical validation confirm that the DPTPTS model improves encryption strength, minimizes latency, and ensures balanced resource utilization across multiple cloud service providers. The use of contextual intelligence (CI) further refines data distribution decisions, enabling dynamic and adaptive performance in real-time scenarios. In future work, this model will be expanded through large-scale deployment and real-time implementation, with an emphasis on developing a fully autonomous trust-aware cloud ecosystem capable of supporting privacy-sensitive applications across sectors such as healthcare, finance, and smart governance.

REFERENCES

1. Murugesan, P., 2025. Security And Privacy Enhancement In Mobile-Cloud Computing Through Cloud Broker Trust Management Implementation Using CITE Frame Work. Cuestiones de Fisioterapia, 54(3), pp.2236-2242.

2. Yang, F., Tian, F., Wu, H., Mou, J., Dong, S. and Lin, M., 2025. Design of Security and Privacy Models for Optimizing the Selection of Cloud Service Providers in Cloud Computing Environments. Scalable Computing: Practice and Experience, 26(2), pp.641-650.

3. A. B. M. B. Alam, Z. M. Fadlullah and S. Choudhury, "A Resource Allocation Model Based on Trust Evaluation in Multi-Cloud Environments," in IEEE Access, vol. 9, pp. 105577-105587, 2021, doi: 10.1109/ACCESS.2021.3100316.

4. Tabassum, N. and Reddyy, C.R.K., 2023. Review on QoS and security challenges associated with the internet of vehicles in cloud computing. Measurement: Sensors, 27, p.100562.

5. Ometov, A., Molua, O.L., Komarov, M. and Nurmi, J., 2022. A survey of security in cloud, edge, and fog computing. Sensors,

22(3), p.927.

6. Aldossary, S. and Allen, W., 2016. Data security, privacy, availability and integrity in cloud computing: issues and current solutions. International Journal of Advanced Computer Science and Applications, 7(4).

7. Wang, J., Li, Z., Liu, H., Qiu, T. and Luo, H., 2025. A Trust-Based Computation Offloading Framework in Mobile Cloud-Edge Computing Networks. IEEE Transactions on Mobile Computing.

8. Suryavanshi, N.S., Acharya, P.S. and Jadhav, A.N., 2025. A Trust-Security-Resource Optimization Framework for Cloud-Edge-IoT Collaboration in Industrial Applications. IJSAT-International Journal on Science and Technology, 16(1).

9. Saini, H., Singh, G., Kaur, A., Saini, S., Wani, N.A., Chopra, V., Akhtar, Z. and Bhat, S.A., 2024. Hybrid Optimization Machine Learning Framework for Enhancing Trust and Security in Cloud Network. IEEE Access.

10. Saini, H., Singh, G. and Rohil, M., 2023. Design of hybrid metaheuristic optimization algorithm for trust-aware privacy preservation in cloud computing. International Journal of Computer Networks and Applications, 10(6), pp.934-946.

11. Dhamdhere, S.D., Sivakkumar, M. and Subramanian, V., 2025. Cloud data security with deep maxout assisted data sanitization and restoration process. High-Confidence Computing, 5(1), p.100238.

12. Chen, S. and Huang, Y., 2025. A privacy-preserving federated learning approach for airline upgrade optimization. Journal of Air Transport Management, 122, p.102693.

13. Yu, Z., Zhang, Y., Guo, C., Sun, Y. and Dai, X., 2025. Application research of improved red tailed eagle algorithm inspired by biomechanics in parameter identification of photovoltaic cells. Molecular & Cellular Biomechanics, 22(3), pp.1118-1118.

14. Shivashankar, M. and Mary, S.A., 2021. Privacy preservation of data using modified rider optimization algorithm: Optimal data sanitization and restoration model. Expert Systems, 38(3), p.e12663.

15. Vanier, K.H. and Balamuruganb, P., 2024. Data Privacy Preservation with Optimization Technique for Effective Multi-Cloud Storage and Security. In Next-Gen Technologies in Computational Intelligence (pp. 129-140). CRC Press.

16. Kesavan, E., 2025. The Impact of Cloud Computing on Software Development: A Review. International Journal of Innovations in Science, Engineering And Management, pp.269-274.

17. Hajlaoui, N., Bejaoui, C., Ismail, T., Ghanmi, H. and Touati, H., 2025. A hybrid architecture for secure data sharing in multi-clouds system. The Computer Journal, 68(1), pp.58-73.

18. Yi, W., Wang, C., Chen, J., Kuzmin, S., Gerasimov, I. and Cheng, X., 2025. DSDM- TCSE: Deterministic storage and deletion mechanism for trusted cloud service environments. Future Generation Computer Systems, 165, p.107611.

19. Wu, Y., Cai, C., Bi, X., Xia, J., Gao, C., Tang, Y. and Lai, S., 2023. Intelligent resource allocation scheme for cloud-edge-end framework aided multi-source data stream. EURASIP Journal on Advances in Signal Processing, 2023(1), p.56.

20. Fernando, N., Shrestha, S., Loke, S.W. and Lee, K., 2025. On Edge-Fog-Cloud Collaboration and Reaping Its Benefits: A Heterogeneous Multi-Tier Edge Computing Architecture. Future Internet, 17(1), p.22.

21. Ojha, S., Paygude, P., Dhumane, A., Rathi, S., Bidve, V., Kumar, A. and Devale, P., 2024. A method to enhance privacy preservation in cloud storage through a three-layer scheme for computational intelligence in fog computing. MethodsX, 13, p.103053.

22. Navale, G.S. and Mali, S.N., 2019. A multi-analysis on privacy preservation of association rules using hybridized approach. Evolutionary Intelligence, pp.1-15