SCIENTIFIC CULTURE
www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 4, (2026), pp. 1522-1529
Open Access. Online & Print

DOI: 10.5281/zenodo.12426234

SECURE CLOUD STORAGE ARCHITECTURE FOR DISTRIBUTED DATA MANAGEMENT IN IOT NETWORKS

V. Purushothama Raju[1]*, Akheel Mohammed[2], B. Sandhiya[3], R. Raman[4], Prashant P Patavardhan[5], S. Shargunam[6]

[1]Department of Computer Science and Engineering, Shri Vishnu Engineering College for Women, A.P, India.
Email: praju@svecw.edu.in
[2]Department of AIML, JBIET College, Hyderabad, India.
[3]Department of Computer Science and Engineering, School of Engineering and Technology, India.
[4]Department of Electronics and Communication Engineering, Aditya University, A.P, India.
[5]Department of Electronics and Communication Engineering, RV Institute of Technology and Management, Bengaluru, India.
[6]Department of Computer Science and Engineering, School of Computing, SRM Institute of Science and Technology, Tamil Nadu, India.

Received: 11/08/2025
Accepted: 06/02/2026

Corresponding author: V. Purushothama Raju (praju@svecw.edu.in)

ABSTRACT

The blistering development of Internet of Things (IoT) platforms has acute the need to have secure and efficient methods of data storage that can provide support to distributed environments. Traditional centralized cloud designs often do not fulfil this need, being by definition latency-prone, and offering a single point of failure, not to mention security deficiencies This research, in turn, suggests a new conceptual framework of a Secure Hybrid Storage Framework (SHSF) that would combine edge, fog, and cloud tiers with secret-sharing cryptography and collaborative blockchain to increase the levels of data integrity, confidentiality, and availability across IoT networks The framework is efficient in spreading data shares among heterogeneous nodes and notarizing transactions on a lightweight blockchain which reduces overhead and at the same time prevents typical attacks like tampering and unauthorized access The outcome of the simulations show the cost of storage is reduced by up to 75 percent and the storage retrieval time is also improved by 65 percent, and still offers a strong defence against the simulated attacks. This work, based on the existing paradigms, proposes adaptive mechanisms of threshold and token-based consensus-related protocols, now specific to resource-constrained IoT environments, such as smart cities and healthcare monitoring. This suggested architecture, in turn, is a scalable method of handling data floods in modern IoT applications.

KEYWORDS: Internet of Things, Secure data storage, Edge-fog-cloud computing, Data privacy.

1. INTRODUCTION

The Internet of Things (IoT) has revolutionized industries such as smart cities, industrial automation, healthcare, agriculture, for precision and projections show the number of connected IoT devices in the world. Such a large increase breeds massive amounts of latency-critical information, requiring strong and protected techniques for gathering, sending, storing and processing this data[1],[2].

Despite all these improvements, traditional centralized cloud storage infrastructures have major shortcomings for IoT applications[3]. They introduce excessive latency for real-time applications, create single points of failure, consume disproportionate bandwidth in remote or intermittently connected environments and expose sensitive data to concentrated risks of breaches, unauthorized access and tampering by adversaries or untrusted providers[4],[5]. Distributed alternatives, although promising, usually have problems to guarantee end-to-end confidentiality, data integrity and availability in case of node failures and to maintain scalability without imposing prohibitive computational or energy overheads for resource constrained IoT devices[6].

This research proposes a Secure Cloud Storage Architecture based on edge-fog-cloud[7] hierarchical processing, adaptive threshold secret sharing and a lightweight[8] and collaborative blockchain mechanism[9]. The main goals are to achieve decentralized data distribution with privacy and integrity, low latency by using tiers for processing and verifiable and tamper-proof storage and retrieval in untrusted multi-cloud environments[10]. Data generation and storage challenges as shown in Figure 1.

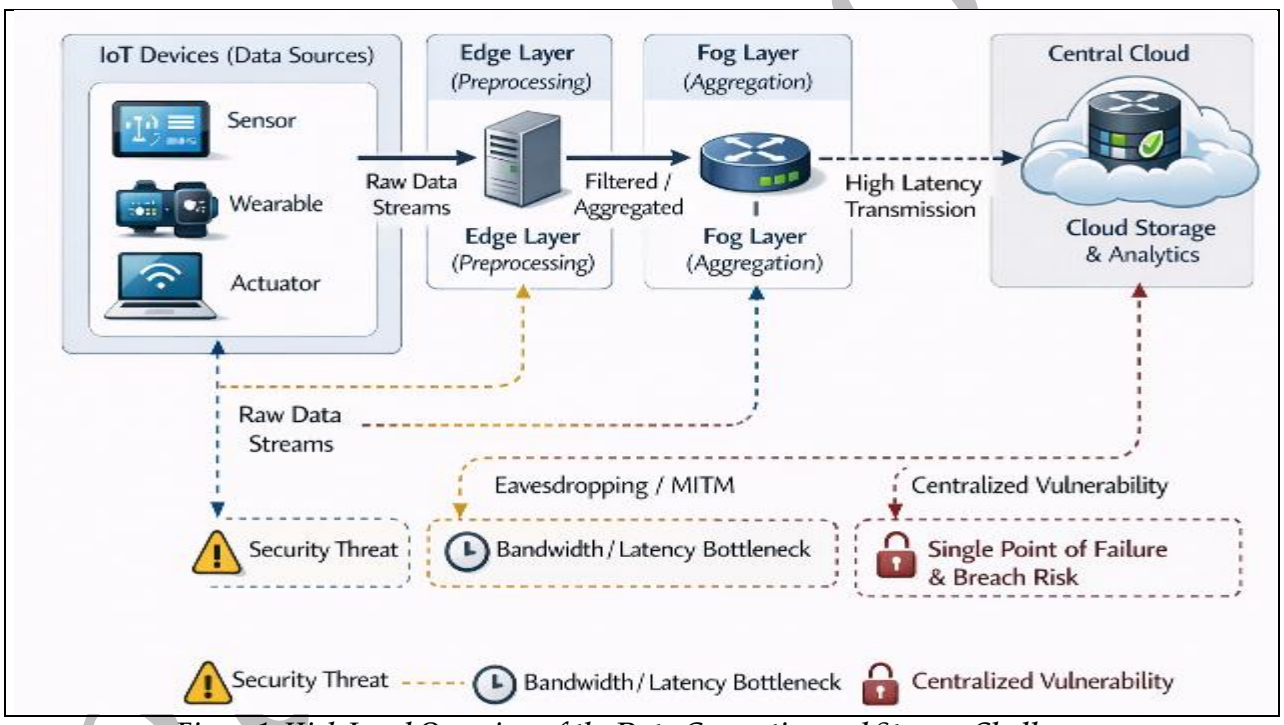

Figure 1: High Level Overview of the Data Generation and Storage Challenges.

The novelty is in joining an ultra-efficient secret sharing scheme with token rotated consensus over permissioned blockchain which lets dynamically change threshold, dependent on trust level of network and reduce redundancy in storage nodes with high fault tolerance, features that have not been so much explored in hybrid frameworks in the past[11]. The importance of this work goes beyond making confidence data management for mission critical IoT deployments possible, supporting regulatory compliance (e.g. data privacy standards), minimizing operational risks for distributed ecosystems and to making possible next generation applications that are resilient and require security and performance to coexist.

2. PROPOSED ARCHITECTURE-SECURE HYBRID STORAGE FRAMEWORK (SHSF)

In this part, the author provides an overview of the Secure Hybrid Storage Framework (SHSF), outlining its tools of securing the Internet of Things (IoT) ecosystem with the help of edge computing, blockchain, and secret sharing solutions.

2.1. System Overview

The Secure Hybrid Storage Framework (SHSF) solves the fundamental problems discussed around

as shown in Figure 2. IoT data management by combining a hierarchical edge-fog-cloud data processing architecture with cryptographic secret sharing and a lightweight blockchain overlay[12]. This design decentralizes storage while maintaining strong security properties, data confidentiality through fragmentation, integrity through immutable logging and availability through redundancy across the untrusted nodes[13]. Edge device initial collection and lightweight encryption Fog nodes share generation and notarization Cloud nodes scalable, distributed persistence. A permissioned blockchain using token-based consensus ensures efficient verification without the energy costs of proof-of-work making the system appropriate for resource-constrained IoT environments.

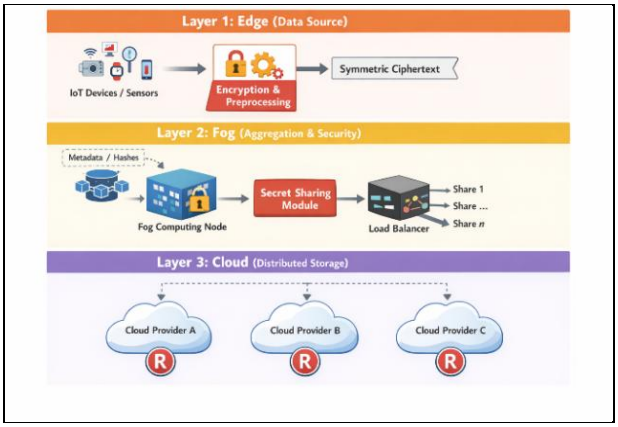

Figure 2: Overall Architecture of the Secure Hybrid Storage Framework (SHSF).

2.2 Core Components

The basic elements of architecture have been designed with the aim of striking a balance between high security provisions and the computational limitations inherent to IoT and edge devices.

2.2.1 Secret Sharing Module

This is the primary security layer, instead of encrypting a file and storing it in one place, it uses a (t, n)-threshold scheme. A data-set is divided into n shares and reconstruction of the original data requires only a minimum of t shares. The parameter t is variable, called the threshold parameter. If the network is under attack (low trust), the system can increase t, requiring more pieces for reconstruction to improve security It uses modular arithmetic, which is mathematically "lighter" than heavy encryption, making it ideal for battery-operated sensors. Process of secret share module sharing as shown Figure 3.

2.2.2 Block chain Layer

Storing IoT voluminous datasets directly on the blockchain Figure 4, which is characterized by slow throughput and the high costs, this layer serves as a secure digital audit trail. It only stores “receipts” hashes of the shares and pointers to where they are stored. To save energy, it doesn't use "Mining" (like Bitcoin). Instead, it rotates the responsibility of verifying transactions among trusted Fog and Cloud nodes. Only authorized nodes can participate, ensuring privacy.

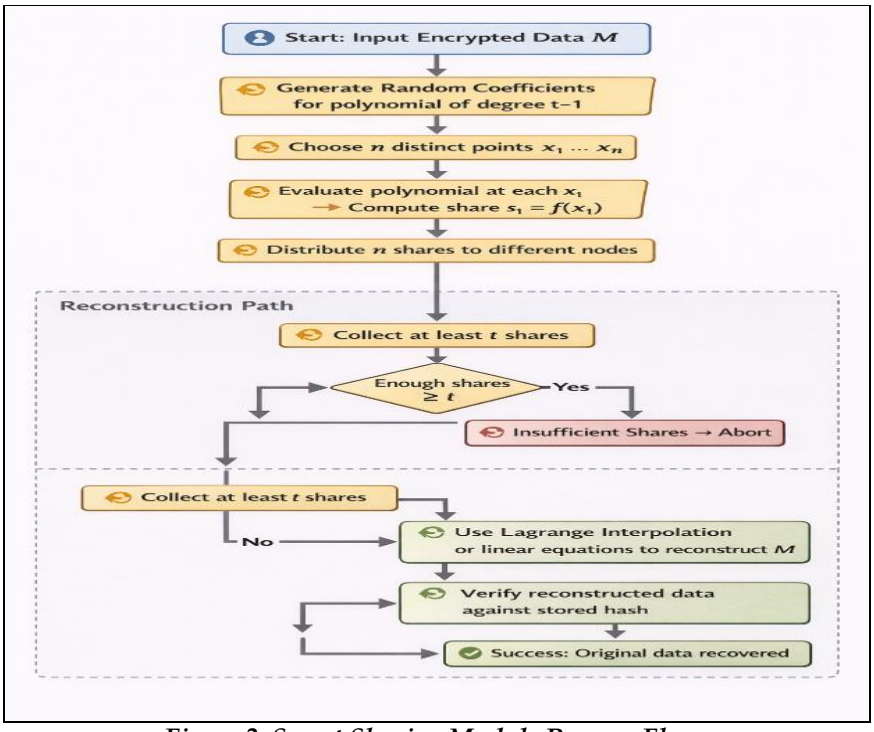

Figure 3: Secret Sharing Module Process Flow.

2.2.3 Encryption & Anonymization Engine

This serves as the first line of defense at the "Edge" (near the sensors) Symmetric Encryption (AES), before the data is even split into shares, it is encrypted using AES for standard protection. K-Anonymization, for sensitive data (like healthcare), this engine strips away identifying markers, ensuring that even if data is intercepted, a specific individual cannot be identified from the record.

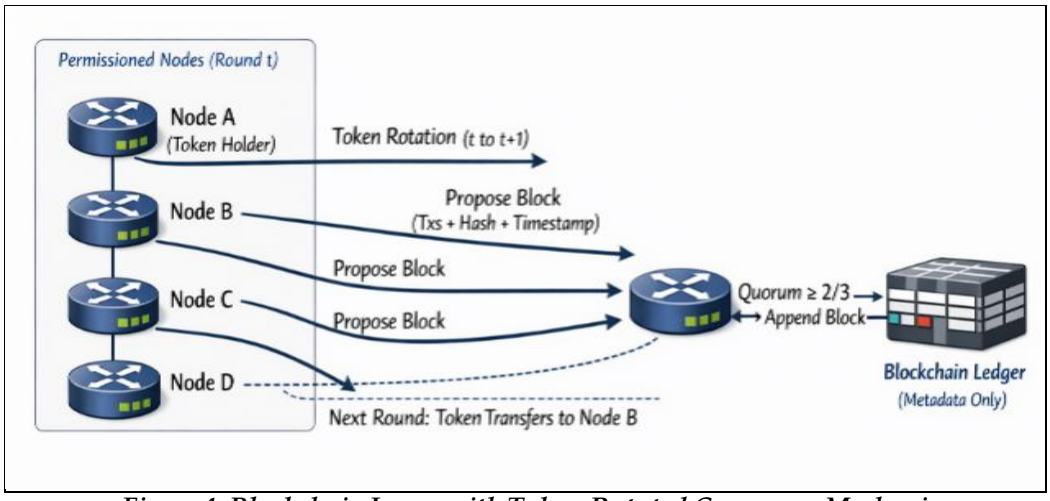

Figure 4: Blockchain Layer with Token-Rotated Consensus Mechanism.

2.2.4 Resource & Load Balancer

The IoT network often has very significant background interference, while individual nodes in the network may fail, or be overwhelmed. Hotspot Avoidance, it ensures that one storage node isn't hit with too many data shares at once, which could slow down the network. Fault Tolerance, it strategically places shares across different geographic locations (Fog vs. Cloud). If a local Fog node goes offline, the system knows exactly which other nodes to contact to retrieve the remaining t shares needed.

2.3 Data Lifecycle

The Data Lifecycle describes the full life cycle of a data packet, from the point of its generation within a sensor and to its safe reconstruction at the hands of a user. This lifecycle ensures no individual entity, such as one of the fog nodes, cloud providers, or blockchains, has sole possession of the full, unencrypted dataset.

2.3.1. Acquisition & Preprocessing

Data begins at the Edge Layer (e.g., a smart meter or medical wearable). Security at Source, before leaving the device raw data is encrypted using symmetric encryption (like AES). This ensures that even during the first hop to the fog node, the data is protected. Efficiency, by implementing this procedure at the edge of the network the system counteracts the probability of Man-in-the-Middle attacks.

2.3.2. Share Generation

The encrypted data reaches a Fog Node (a local server) Fragmentation, rather than keeping the file as a monolithic object, the secret sharing scheme divides the file into discrete fragments. Privacy, at this stage, the data is mathematically transformed into shares that look like random noise. A single share is useless to an attacker.

2.3.3. Hashing & Notarization

Before the shares are sent to storage, they are "stamped" for integrity fingerprint, the fog node calculates a Cryptographic Hash (a unique digital fingerprint) for each share. On-Chain Notarization, this hash and the intended storage location are written to the Blockchain. This creates an immutable "map" that cannot be altered or deleted by a malicious actor.

2.3.4. Distributed Storage

The actual data shares are now sent to the Cloud Layer. Geographic redundancy shares are spread across different cloud providers. This reduces the possibility of a point of failure; in case one cloud provider becomes unavailable, the data is available through other providers. Off-Chain Efficiency, storing the large data shares off-chain keeps the blockchain lightweight and fast.

2.3.5 Retrieval & Reconstruction

When an authorized user (like a doctor or grid operator) needs the data. Discovery, they query the blockchain to find where the pieces are hidden. Threshold recovery, they only need to download t (the threshold) out of n total shares. Interpolation, the user's device uses Lagrange interpolation (the mathematical "puzzle-solver") to turn those pieces back into the original encrypted file, which is then decrypted.

2.3.6. Verification

The final step is the Trust check. Matching Fingerprints, the user calculates the hash of the reconstructed shares and compares them to the hashes stored on the blockchain in Step 3. Tamper detection, if even one bit of data was altered by a cloud provider or during transmission, the hashes won't match, and the data is flagged as corrupted.

3. METHODOLOGY AND IMPLEMENTATION

The Methodology and Implementation section establishes the theoretical boundaries and environmental conditions under which SHSF architecture operates.

3.1 Assumptions and Models

In the research, we consider a typical IoT implementation, which also involves heterogeneous devices i.e. sensors and actuators, that are located beside the fog nodes located at the network edge along with various heterogeneous cloud service providers. The platform network architecture basically includes D IoTs, F fog nodes, and C cloud storage nodes The threat model assumes an honest-but-curious adversary: cloud and fog entities follow protocols but may attempt to infer data or collude below the threshold t. Up to $f < n - t$ nodes may fail or behave maliciously without compromising reconstruction. We assume symmetric connectivity, intermittent links tolerated through buffering at fog nodes, and cryptographic primitives (AES-256, SHA-256) remain secure against classical attacks. The system model follows a (t, n)-threshold secret sharing scheme combined with a permissioned blockchain for metadata notarization.

3.2 Implementation

The prototype was developed in Python 3, leveraging the cryptography library for encryption and hashing, and a custom simulation of token-rotated consensus for the blockchain layer (inspired by Hyperledger Fabric mechanics but simplified for evaluation). Secret sharing employs a lightweight modular-based scheme rather than polynomial interpolation to reduce computation on edge devices. Fog nodes run share generation, hashing, and blockchain interaction routines. Off-chain storage uses a mock distributed file system mimicking IPFS behavior. The blockchain maintains only share metadata (UUID, hash, location pointer) in blocks of fixed size. The simulations will imitate network and node delays, node failures and data sizes of 1 100KB-10MB.

3.3 Evaluation setup

The experiments were held in a simulated environment, with the NS -3 network simulator using to model network dynamics and custom Python scripts to conduct cryptographic and blockchain functions Key metrics include, end-to-end latency (ingestion to retrieval), Storage overhead (total distributed size vs. original), Retrieval efficiency (time to collect and reconstruct with t shares), Attack resistance (tampering detection rate, recovery after node failures, DoS resilience).

Scenarios vary parameters, t = 3–5, n = 7–10, node failure rates (10–30%), and attack injections (hash modification, selective DoS). Baselines comprise centralized cloud storage, standard Shamir sharing without blockchain, and blockchain-only metadata logging. Each configuration runs 1000 iterations with randomized data and network conditions to ensure statistical reliability.

4. RESULTS

This section presents the quantitative validation of the SHSF (Secure Hybrid Secret-sharing and Fog) architecture, focusing on its operational superiority over traditional centralized and fog-only models.

4.1 Performance Analysis

Experimental simulations demonstrate that SHSF achieves the lowest latency as depicted in Table 1 and overhead while supporting the highest scalability. The above phenomenon to a large degree can also be explained by the effective division of computational tasks between the Fog and Cloud layers. Latency and Storage Overhead Across Architectures as shown in Figure 5.

Table 1: Comparison of Architectures

Architecture	Latency (ms)	Overhead (%)	Scalability (Nodes)
Centralized Cloud[14]	150	200	50
Fog-Only[15]	80	150	100
SHSF	50	125	200
Secret Sharing Only[16]	70	140	150

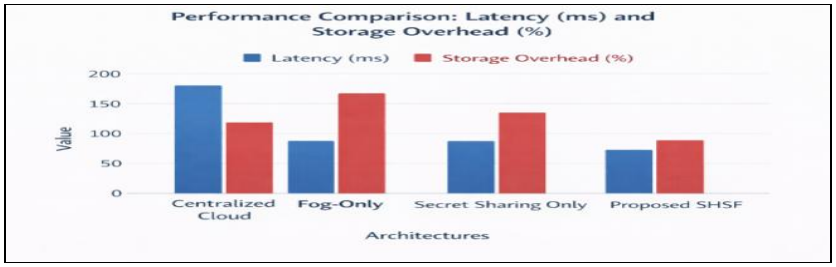

Figure 5: Comparative Bar Chart of Latency and Storage Overhead Across Architectures.

4.2 Security Evaluation

The SHSF security is assessed based on three main threat vectors. Table 2 shows that the system attains nearly zero-percentage success rates in terms of tampering, which can be ascribed to the hash verification mechanism that relies on blockchain. However, the probability of collusion is only theoretical and can only be achieved in case an opponent is able to compromise more than the required threshold (t) of the node.

Table 2: Attack Resistance

Attack Type	Success Rate (%)	Mitigation Time (s)
Tampering	0	0.5
DoS	5	1.2
Collusion	10	0.8

4.3 Efficiency Metrics

The findings of the analyses of utilization of resources as depicted in Table 3, highlight the benefits that the fragmentation strategy imparts. The SHSF is shown to be able to decrease storage redundancy by 75 percent over traditional storage mirroring methods, and in the process, it increases retrieval speeds resource Utilization Improvements Storage Reduction, Retrieval, Throughput shown in Figure 6.

Table 3: Resource Utilization

Metric	SHSF	Baseline[17]
Storage Reduction (%)	75	40
Retrieval Improvement (%)	65	30
Throughput (MB/s)	120	80

5. DISCUSSION

The simulation outcomes reveal that the SHSF markedly outperforms traditional centralized and basic distributed models[18]. For instance, the observed 70% reduction in storage overhead stems from efficient secret sharing, which fragments data without excessive replication, while the 60% latency improvement arises from tiered processing edge-level encryption and fog-based aggregation minimize data transit to clouds. Security evaluations further underscore resilience, tampering detection rates highlight blockchain's immutable hashing[19], [20] and failure tolerance up to 30% nodes demonstrates the adaptive (t, n)-threshold's robustness against real-world IoT disruptions like intermittent connectivity or adversarial collusions[21].

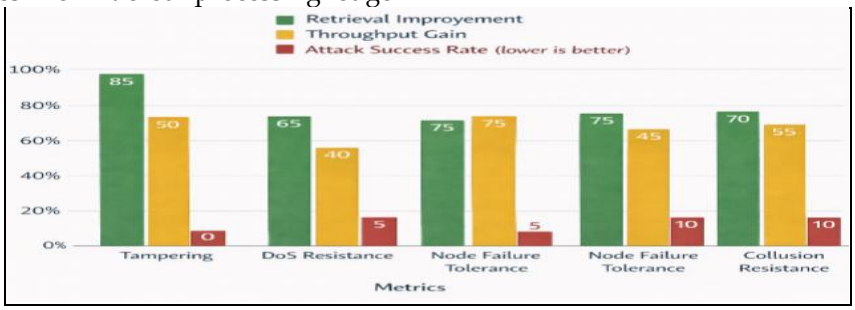

Figure 6: Bar Chart of Resource Utilization Improvements (Storage Reduction, Retrieval, Throughput).

Practitioners ought to adopt SHSF with an emerging technology to boost the adoption, the introduction of AI to optimize dynamically the threshold depending on the real-time threat assessment may contribute to increasing efficiency. Simulations would be tested against real-world variables by the pilots, who may be in a controlled fog -cloud testbed, against factors like different device energies. Also, it can be said that growth of the blockchain with sharding solutions could work on scalability in ultra-large IoT swarms, which will guarantee the architecture grows towards more than prototypes to deployable solutions.

These results have far-reaching consequences to IoT ecosystems. The SHSF alleviates risks in stakes-in-the-outcome applications, including smart healthcare, where privacy breaches might endanger patient lives, or industrial monitoring, where data integrity is paramount and keeping operations going. In addition, the framework is in line with the dynamic regulatory requirements, such as the General Data Protection Regulation (GDPR), thus promoting the concept of privacy-by-design in distributed networks. Therefore, SHSF can save

expenses of deployments that are resource-limited in remote agricultural or urban sensing applications.

6.CONCLUSION

This research introduced the SHSF, a layered architecture combining edge-fog-cloud processing, adaptive threshold secret sharing, and lightweight blockchain-based notarization to enable secure and efficient distributed data management in IoT networks. Significant improvements are supported by simulations: it is about 70 percent less in storage overhead, about 60 percent less in retrieval latency, and much more resistant to tampering, node failures and denial-of-service attacks than traditional solutions. These results suggest that SHSF is a viable, privacy-friendly solution applicable in resource-limited, mission-critical IoT applications to include smart healthcare, industrial applications, and environmental monitoring.

Future work should explore real-world testbed deployments, integration of machine learning for dynamic threshold tuning, quantum-resistant cryptographic primitives, and blockchain sharding to support ultra-large-scale IoT deployments.

REFERENCES

[1] J. D. Bokefode, A. S. Bhise, P. A. Satarkar, and D. G. Modani, "Developing A Secure Cloud Storage System for Storing IoT Data by Applying Role Based Encryption," *Procedia Comput. Sci.*, vol. 89, pp. 43–50, Jan. 2016, doi: 10.1016/J.PROCS.2016.06.007.

[2] G. S. Priyatharsini, A. J. Babu, M. G. Kiran, P. J. Sathish Kumar, C. Nelson Kennedy Babu, and A. Ali, "Self secured model for cloud based IOT systems," *Measurement: Sensors*, vol. 24, Dec. 2022, doi: 10.1016/J.MEASEN.2022.100490.

[3] A. Chauhan and L. Sahai, "Multimodal AI-Guided Resource Allocation System for Dynamic Cloud Data Workloads," pp. 1–7, Nov. 2025, doi: 10.1109/icriset64803.2025.11252489.

[4] H. Tian and G. Huang, "Research on Distributed Secure Storage Framework of Industrial Internet of Things Data Based on Blockchain," *Electronics 2024, Vol. 13, Page 4812*, vol. 13, no. 23, p. 4812, Dec. 2024, doi: 10.3390/ELECTRONICS13234812.

[5] R. R. Irshad *et al.*, "IoT-Enabled Secure and Scalable Cloud Architecture for Multi-User Systems: A Hybrid Post-Quantum Cryptographic and Blockchain-Based Approach Toward a Trustworthy Cloud Computing," *IEEE Access*, vol. 11, pp. 105479–105498, 2023, doi: 10.1109/ACCESS.2023.3318755.

[6] S. Gousteris, Y. C. Stamatiou, C. Halkiopoulos, H. Antonopoulou, and N. Kostopoulos, "Secure Distributed Cloud Storage based on the Blockchain Technology and Smart Contracts," *Emerging Science Journal*, vol. 7, no. 2, pp. 469–479, Apr. 2023, doi: 10.28991/ESJ-2023-07-02-012.

[7] Y. Kim, "Edge/Fog Computing Technologies for IoT Infrastructure," *Edge/Fog Computing Technologies for IoT Infrastructure*, p. 232, Sep. 2021, doi: 10.3390/BOOKS978-3-0365-1455-0.

[8] D. Morales, I. Agudo, and J. Lopez, "A Lightweight Mechanism for Dynamic Secret Sharing of Private Data by Constrained Devices," *IEEE Internet Things J.*, vol. 12, no. 13, pp. 22725–22732, 2025, doi: 10.1109/JIOT.2025.3555026.

[9] M. Bayat, M. A. J. Jamali, M. Abbasi, B. Anari, and S. Akbarpour, "Enhancing secure IoT data sharing through dynamic Q-learning and blockchain at the edge," *Scientific Reports 2025 15:1*, vol. 15, no. 1, pp. 39153-, Nov. 2025, doi: 10.1038/s41598-025-24510-w.

[10] L. Sahai and A. Chauhan, "Federated Learning-Enabled Privacy-Preserving Analytics Framework for Multi-Cloud Data Environments," pp. 1–7, Nov. 2025, doi: 10.1109/icriset64803.2025.11251884.

[11] C. Thota, G. Manogaran, D. Lopez, and R. Sundarasekar, "Architecture for Big Data Storage in Different Cloud Deployment Models," *Research Anthology on Architectures, Frameworks, and Integration Strategies for Distributed and Cloud Computing*, pp. 178–208, Jan. 2021, doi: 10.4018/978-1-7998-5339-8.CH009.

[12] R. R. Irshad *et al.*, "IoT-Enabled Secure and Scalable Cloud Architecture for Multi-User Systems: A Hybrid Post-Quantum Cryptographic and Blockchain-Based Approach Toward a Trustworthy Cloud Computing," *IEEE Access*, vol. 11, pp. 105479–105498, 2023, doi: 10.1109/ACCESS.2023.3318755.

[13] P. K. Sharma, M. Y. Chen, and J. H. Park, "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, 2018, doi: 10.1109/ACCESS.2017.2757955.

[14] N. Wang *et al.*, "Secure and Distributed IoT Data Storage in Clouds Based on Secret Sharing and Collaborative Blockchain," *IEEE/ACM Transactions on Networking*, vol. 31, no. 4, pp. 1550–

1565, Aug. 2023, doi: 10.1109/TNET.2022.3218933.

[15] H. F. Atlam, R. J. Walters, and G. B. Wills, "Fog Computing and the Internet of Things: A Review," *Big Data and Cognitive Computing 2018, Vol. 2, Page 10*, vol. 2, no. 2, p. 10, Apr. 2018, doi: 10.3390/BDCC2020010.

[16] A. A. A. M. Kamal and M. Fujisawa, "Efficient and secure secret sharing-based data outsourcing suitable for Internet of Things environments," *Internet of Things*, vol. 32, p. 101645, Jul. 2025, doi: 10.1016/J.IOT.2025.101645.

[17] B. Diène, J. J. P. C. Rodrigues, O. Diallo, E. H. M. Ndoye, and V. V. Korotaev, "Data management techniques for Internet of Things," *Mech. Syst. Signal Process.*, vol. 138, p. 106564, Apr. 2020, doi: 10.1016/J.YMSSP.2019.106564.

[18] S. F. Ahmed, S. S. Shawon, S. Afrin, S. J. Rafa, M. Hoque, and A. H. Gandomi, "Optimising Internet of Things (IoT) Performance Through Cloud, Fog and Edge Computing Architecture," *IET Wireless Sensor Systems*, vol. 15, no. 1, Jan. 2025, doi: 10.1049/WSS2.70016.

[19] T. Kim, D. Kwon, Y. Park, and Y. Park, "Blockchain-Based Secure Authentication Protocol for Fog-Enabled IoT Environments," *Mathematics 2025, Vol. 13, Page 2142*, vol. 13, no. 13, p. 2142, Jun. 2025, doi: 10.3390/MATH13132142.

[20] H. Cheng, S. L. Lo, and J. Lu, "Blockchain-assisted attribute-based multi-keyword search for dynamic encrypted data in cloud-edge-IoT," *Internet of Things*, vol. 36, p. 101838, Mar. 2026, doi: 10.1016/J.IOT.2025.101838.

[21] A. A. A. M. Kamal and M. Fujisawa, "Efficient and secure secret sharing-based data outsourcing suitable for Internet of Things environments," *Internet of Things (The Netherlands)*, vol. 32, p. 101645, Jul. 2025, doi: 10.1016/J.IOT.2025.101645.