International Journal of Advanced Research in Science, Engineering and Technology

ISSN: 2350-0328

IJARSET IMPACT FACTOR 7.150

Vol. 13, Issue 2, February 2026

An Exploratory Study of Privacy-Preserved Multi-Cloud Storage with Automated Security Bots

M.Dancily Jebamalar, Dr.J. Anthoniraj

Research Scholar, PG & Research Department of Computer Science, Jamal Mohamed College (Autonomous), (Affiliated to Bharathidasan University), Trichy – 620020.
Research Supervisor, Assistant Professor, Department of Computer Science, Jamal Mohamed College (Autonomous), (Affiliated to Bharathidasan University), Trichy – 620020.

ABSTRACT: Cloud storage services have transformed modern computing, but they also raise profound privacy and security challenges. Multi-cloud storage mitigates single provider risks by distributing data across independent service providers. However, preserving privacy while ensuring data integrity, confidentiality, and secure access control remains unsolved. This paper presents an advanced theoretical exploration of privacy-preserving multi-cloud storage systems enhanced with automated security bots. The proposed architectural framework integrates cryptographic primitives, federated learning, blockchain-based auditing, and autonomous AI defenses to provide a comprehensive security ecosystem. We formalize the threat model, propose modular solutions, and analyze security guarantees. The results illuminate trade-offs between privacy, scalability, and performance, and pave the way for resilient, adaptive cloud storage infrastructures.

KEYWORDS: Privacy Preservation, Multi-Cloud Storage, Automated Security Bots, Blockchain, Federated Learning, Homomorphic Encryption, Secure Data Outsourcing.

I. INTRODUCTION

Cloud computing has enabled scalable on-demand computing and storage. Enterprises from healthcare to finance depend on cloud platforms to store sensitive user data. Despite its benefits, centralized cloud platforms remain vulnerable to insider threats, data breaches, and single points of failure. Multi-cloud storage — distributing data fragments across multiple service providers — offers enhanced availability and resilience, but introduces complex privacy challenges.

Recent studies (e.g., Zhang *et al.*, [1]; Song *et al.*, [2]) have proposed trust-based frameworks and secure data sharing mechanisms, but they often lack adaptive threat mitigation and robust privacy guarantees. This study addresses these gaps by integrating:

- Threshold cryptography and secure multi-party protocols
- Federated learning for distributed anomaly detection
- Block chain-based tamper-proof auditing
- Automated AI-driven security bots

The contribution of this work is a **holistic theoretical model** for privacy-preserving multi-cloud storage with verifiable security guarantees.

II. BACKGROUND AND MOTIVATION

A. Privacy Challenges in Cloud Storage

Data confidentiality, integrity, and controlled sharing are central to cloud privacy. Traditional encryption ensures data secrecy, but complicates efficient querying, searching, and computation (e.g., homomorphic evaluation). Moreover, cross-cloud correlation and side-channel attacks can reveal sensitive metadata.

B. Multi-Cloud Storage

Multi-cloud storage divides data across n providers C1,...,CnC_1, ..., C_nC1,...,Cn, reducing dependency on any single provider. Threshold schemes such as Shamir's Secret Sharing can reconstruct data only with at least ttt fragments, thereby countering collusion up to t−1t−1t−1 compromised clouds.

C. Autonomous Security Bots

Automated security bots are intelligent agents embedded within each cloud instance. They continuously monitor system behavior, perform anomaly detection, and adapt defense strategies based on federated learning.

III. SYSTEM ARCHITECTURE

We propose a layered architecture:

- **Data Fragmentation & Encryption Layer** – follows (t,n)(t, n)(t,n) threshold sharing, then encrypts fragments.
- **Distributed Storage Layer** – fragments are stored across independent clouds.
- **Integrity Blockchain Layer** – stores integrity proofs (hashes) for each fragment.
- **Security Bot Layer** – federated anomaly detection and mitigation.

A. Data Fragmentation

Let DDD be user data. After threshold splitting:
D→{D1,...,Dn}D \rightarrow \{D_1, ..., D_n\}D→{D1,...,Dn}
Only any ttt fragments reconstruct DDD. Mutual information between partial fragments <t< t<t and DDD is zero.

B. Encryption

Each fragment is encrypted using an IND-CPA secure scheme:
E(Di)=Encpk(Di)E(D_i) = Enc_{pk}(D_i)E(Di)=Encpk(Di)
Security ensures adversaries cannot distinguish ciphertexts.

C. Blockchain Auditing

Hash values Hi=Hash(E(Di))H_i = Hash(E(D_i))Hi=Hash(E(Di)) are recorded in a blockchain ledger. Immutability guarantees tamper detection.

IV. THREAT MODEL

Adversary capabilities:

- Compromise up to kkk clouds, where k<tk < tk<t
- Observe inter-cloud metadata
- Launch adaptive malware and side-channel attacks
- Attempt federated model poisoning

Security definitions:

- **Confidentiality:** Data remains secret unless adversary obtains ≥ t fragments.
- **Integrity:** Any modification of stored fragments is detectable via blockchain.
- **Availability:** Data retrievable under bounded cloud failures.
- **Adaptive Resilience:** Security bots maintain detection convergence in dynamic threats.

V. AUTOMATED SECURITY BOTS FRAMEWORK

Each bot BiB_iBi monitors:

- Access patterns
- API calls
- Latency anomalies
- Traffic correlations

A. Federated Learning Model

Each bot trains a local model WiW_iWi based on local observations.
Global aggregation:
W(t+1)=∑i=1nNiNWiW^{(t+1)} = \sum_{i=1}^n \frac{N_i}{N} W_iW(t+1)=i=1∑nNNiWi
where NiN_iNi is local dataset size.

B. Anomaly Detection

Each bot computes an anomaly score:
fθ(X)=α·IPvariance+β·RequestFreq+γ·AuthFailuresf_\theta(X) = \alpha \cdot IP_{variance} + \beta \cdot RequestFreq + \gamma \cdot AuthFailuresfθ(X)=α·IPvariance+β·RequestFreq+γ·AuthFailures
If fθ(X)>δf_\theta(X) > \deltafθ(X)>δ, a threat is flagged.

C. Adaptive Response

Once a threat is detected, bots can:

- Block suspicious requests
- Quarantine affected fragments
- Trigger re-encryption and re-distribution
- Report to block chain for audit logs

VI. SECURITY ANALYSIS

A. Confidentiality Proof

If adversary compromises k<tk < tk<t providers, then:
Pr[D reconstructed]≤2−mPr[D \text{ reconstructed}] \le 2^{-m}Pr[D reconstructed]≤2−m
since partial fragment information provides no advantage beyond random guessing.

B. Integrity

Cryptographic hash collision resistance ensures:
Hash(E(Di))stored≠Hash(E(Di′))modifiedHash(E(D_i))_{stored}\neq Hash(E(D_i'))_{modified}
Hash(E(Di))stored=Hash(E(Di′))
modified with negligible probability.

C. Adaptive Robustnes

Under bounded model poisoning, convergence of federated models is guaranteed if learning rate η<1L\eta < \frac{1}{L}η<L1, where LLL is Lipschitz constant of the loss surface.

VII. PERFORMANCE AND COMPARATIVE ANALYSIS

We analyze four security dimenions:

Security Mechanism	**Encryption**	**Access Control**	**Privacy**	**Scalability**
Threshold + Encryption	High	Moderate	High	Moderate
Blockchain	Moderate	High	High	Moderate
Federated Bots	Moderate	Adaptive	High	High
Homomorphic Encryption	Very High	High	Very High	Low

Observation: A hybrid model combining all four provides balanced security and scalability.

VIII. RESEARCH CHALLENGES

Key challenges remain:

- Reducing homomorphic encryption overhead
- Securing federated learning against poisoning
- Managing key lifecycles
- Cross-cloud identity federations

- Efficient blockchain throughput

IX. FUTURE DIRECTIONS

Future work includes:

- Zero-knowledge proof integration for stronger privacy
- Quantum-resistant cryptographic primitives
- Risk-aware federation policies
- Explainable AI for security bots
- Secure gradient aggregation schemes

X. CONCLUSION

By integrating distributed cryptographic primitives, federated learning, and blockchain auditing, this architecture enhances confidentiality, integrity, and availability under diverse threats. This paper outlines theoretical foundations and future research pathways for robust, secure multi-cloud environments.

XI. REFERENCES

[1] J. Zhang, T. Li, Z. Ying and J. Ma, “Trust-Based Secure Multi-Cloud Collaboration Framework in Cloud-Fog-Assisted IoT,” IEEE Trans. Cloud Comput., vol. 11, no. 2, pp. 1546–1561, 2023.

[2] Z. Song, H. Ma, R. Zhang, W. Xu and J. Li, “Secure Data Sharing Mechanism for Cloud-Edge Computing,” IEEE Trans. Inf. Forensics Sec., vol. 18, pp. 2234–2249, 2023.

[3] T. Li, J. Chu and L. Hu, “CIA: Collaborative Integrity Auditing for Cloud Data with Multi-Replica on Multi-Cloud Providers,” IEEE Trans. Parallel Distrib. Syst., vol. 34, no. 1, pp. 154–162, 2023.

[4] F. Rezaeibagha, Y. Mu, K. Huang, L. Chen and L. Zhang, “Toward Secure Data Computation and Outsource for Multi-User Cloud-Based IoT,” IEEE Trans. Cloud Comput., vol. 11, no. 1, pp. 217–228, 2023.

[5] K. Hu, S. Gong, Q. Zhang, C. Seng and M. Xia, “An Overview of Implementing Security and Privacy in Federated Learning,” Artif. Intell. Rev., vol. 57, no. 2, 2024.

[6] S. A. Mahmud et al., “Privacy-Preserving Federated Learning-Based Intrusion Detection Technique for Cyber-Physical Systems,” Mathematics, vol. 12, no. 20, 3194, 2024.

[7] G. Rampone, T. Ivaniv and S. Rampone, “Hybrid Federated Learning Framework for Privacy-Preserving Intrusion Detection in IoT,” Electronics, vol. 14, no. 7, 1430, 2025.

[8] L. Albshaier, S. Almarri and A. Albuali, “Federated Learning for Cloud and Edge Security: Challenges and AI Opportunities,” Electronics, vol. 14, no. 5, 1019, 2025.

[9] K. N. Mishra, R. K. Lal, P. N. Barwal and A. Mishra, “Advancing Data Privacy in Cloud Storage: Multi-Layer Encoding Framework,” Appl. Sci., vol. 15, no. 13, 7485, 2025.

[10] “Security and Privacy in Multi-Cloud and Hybrid Cloud Environments: Challenges, Strategies, and Future Directions,” Comput. Secur., vol. 157, 104599, 2025.

[11] “Cloudlock: Secure Data Sharing Using a Hybrid Cryptosystem in Multi-Cloud Storage,” Cluster Comput., vol. 28, art. 464, 2025.

[12] B. D. Manh et al., “Homomorphic Encryption-Enabled Federated Learning for Privacy-Preserving Intrusion Detection in Resource-Constrained Networks,” arXiv, 2024.

[13] J. Shen et al., “Effective Intrusion Detection in Heterogeneous Networks via Ensemble Knowledge Distillation-Based Federated Learning,” arXiv, 2024.

[14] S. Rawas and A. D. Samala, “Dual-Layer Security Framework for Privacy Preserving AI-Driven Healthcare Edge Cloud Analytics,” Discov. Netw., 2025.

[15] A. Kumar B. R., “Data Privacy on Multi-Cloud using Blockchain Smart Contract and Zero Knowledge Proof,” Int. J. Intell. Syst. Appl. Eng., vol. 12, no. 4, 3631, 2024.

[16] A. K. Awais and A. Adeel, “Secure Parking Recommender Using ECC and Local Differential Privacy,” IEEE Access, 2022.

[17] S. Zaman and R. A. K. Muhammad, “Holochain for Distributed Security in IoT Healthcare,” IEEE Access, 2022.

[18] J. Liu et al., “Multi-Keyword Ranked Searchable Encryption with Wildcard Keywords in Cloud Computing,” Comput. J., vol. 66, no. 1, pp. 184–196, Jan. 2023.

[19] J. Cui et al., “Bidirectional Access Control for Cloud-Edge Data Sharing,” IEEE Trans. Parallel Distrib. Syst., vol. 33, no. 2, pp. 476-488, 2022.

[20] S. Sun et al., “WebCloud: Secure Cross-Platform Data Sharing,” IEEE Trans. Dependable Secure Comput., vol. 19, no. 3, pp. 1871-1884, 2022.

[21] J. Hao et al., “Secure Data Sharing with Flexible Privilege Updates in Cloud-Assisted IoMT,” IEEE Trans. Emerg. Topics Comput., vol. 10, no. 2, pp. 933-947, 2022.

AUTHOR'S BIOGRAPHY

Full name	**M.Dancily Jebamalar**
Academic rank	Research Scholar
Institution	PG & Research Department of Computer Science, Jamal Mohamed College (Autonomous), (Affiliated to Bharathidasan University), Trichy – 620020

Full name	**Dr.J. Anthoniraj**
Academic rank	Research Supervisor , Assistant Professor
Institution	Department of Computer Science, Jamal Mohamed College (Autonomous), (Affiliated to Bharathidasan University), Trichy – 620020