iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VIII **Month of publication:** August 2025

DOI: https://doi.org/10.22214/ijraset.2025.73918

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VIII Aug 2025- Available at www.ijraset.com

Computational Intelligence Enabled Three-Layer Privacy Preserving Cloud Storage for Fog Computing

Mr. Md Saquib Ahmed S[1], Mrs. Jennifer Mary S[2]
[1]*Assistant Professor, Department of MCA, Ballari Institute of Technology &Management, Ballari, Karnataka, India*
[2]*Department of MCA, Ballari Institute of Technology &Management, Ballari, Karnataka, India*

Abstract: ***Over the past few years, cloud computing has witnessed remarkable growth and evolution. The rapid expansion of formless data is driving greater research and attention to cloud storage technology. But according to the present storage structure, within existing storage models, user data is fully concentrated in cloud servers, which results in users gradually losing direct authority over their information and facing higher risks of privacy breaches. Conventional privacy safeguards primarily rely on encryption, yet such methods fall short when it comes to mitigating insider threats within cloud service environments. We suggest a fog computing- To address this concern, a layered storage framework leveraging fog computing is proposed. The suggested architecture can safeguard data privacy while utilizing cloud storage to its fullest potential. Additionally, The Hash-Solomon coding mechanism is employed to break data into multiple independent fragments. To preserve anonymity, we can then save a small subset of the data is stored across the user's device and nearby fog servers. Further-more, through computational intelligence, the system dynamically determines how data should be allocated among the local device, fog nodes, and cloud servers. The viability of our plan, which is a very potent addition to the current cloud storage scheme, has been confirmed by the both security-focused theoretical studies and practical experiments validate the effectiveness of this approach.***
Keywords: Three-Layer Privacy Preserving, Cloud Storage, Fog Computing

I. INTRODUCTION

Since the beginning of the 21st century, computer technology has progressed at an accelerated pace. The on-demand technology known as cloud computing was first introduced in San Jose, it has become highly attractive across multiple sectors of society. Cloud storage is a key component of cloud-based technologies. The rapid expansion of networking has caused user data to grow exponentially, surpassing the storage capacity of local machines. Thus, people attempt must discover fresh ways to keep their data in more potent storage spaces, where many users opt for cloud storage. In addition to offering data management and storage services, cloud storage technology is the future technology. With the use of network and distributed file system technologies, cloud storage enables numerous storage devices to cooperate.

Many businesses offer a range of cloud storage services, like Google Drive, iCloud, and others. Such providers attract a large user base by delivering massive storage capacity along with diverse service offerings. Additionally, services for cloud storage have numerous security issues. Among the major security challenges, safeguarding privacy remains critical.

Here, users transfer their files directly to the cloud, where the Cloud Service Provider (CSP) takes complete responsibility for managing it. The data saved in the cloud can be freely searched and accessed by CSP, but attackers can also target the CSP server to steal user data. Thus, the two examples above cause users to loss of data and disclosure of information.

The majority of issues can be resolved by using data encryption, which is the main focus of traditional secure cloud storage solutions. However, internal attacks cannot be resolved by any of these approaches. To get around this, we create a Hash-Solomon code based on the Reed-Solomon code and suggest a TLS strategy based on the fog computing concept. Fog computing, an extended computing architecture based on cloud computing, is made up of numerous fog nodes with processing and storage capabilities. According to our plan, user data is categorized into three sections and saved independently on the user's local computer, the cloud server, and the fog server. Depending on the Hash-Solomon code's properties, which guarantee that partial data can't be utilized to recuperate the original data and generate some similar data blocks for the decoding process. Increasing the amount of redundant blocks leads to more data storage while also improving storage dependability. Multifaceted calculations are required for hash-Solomon code, and computational intelligence (CI) helps with this.

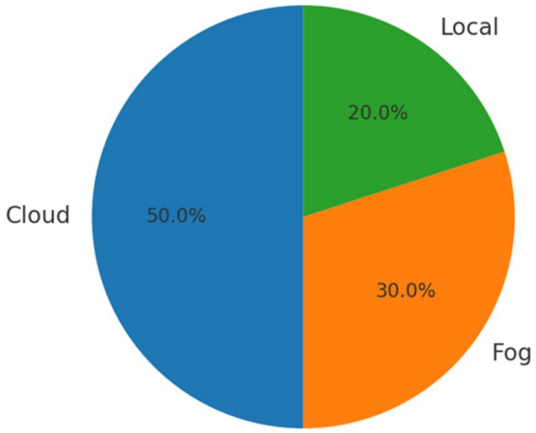


Fig. Data distribution across Cloud, Fog, and Local storage.

II. PROBLEM STATEMENT

A rising number of people and businesses are outsourcing their data to third-party providers for affordable and scalable storage due to the quick uptake of cloud storage. But there are significant privacy and security hazards associated with this convenience. Cloud-based sensitive data is susceptible to misuse, data breaches, and illegal access by both internal and external adversaries. The usability of cloud-based services is limited by the fact that, although helpful, traditional encryption solutions frequently don't allow flexible data exchange and calculation without disclosing the contents. Furthermore, once data is uploaded, Once the data is uploaded, users generally lose direct authority over it, creating concerns regarding reliability and trust. Creating a cloud storage system that strikes a balance between data usefulness and privacy protection is the main challenge. For safe data exchange, access control, and privacy protection, the system must provide dynamic, intelligent decision-making. It is anticipated that the use of computational intelligence would provide context-aware, adaptive security methods that surpass static rule-based approaches. As a result, forming a secure storage protocol is one of the challenges; another is integrating intelligent analytics and learning features that change in response to new threats and use trends.

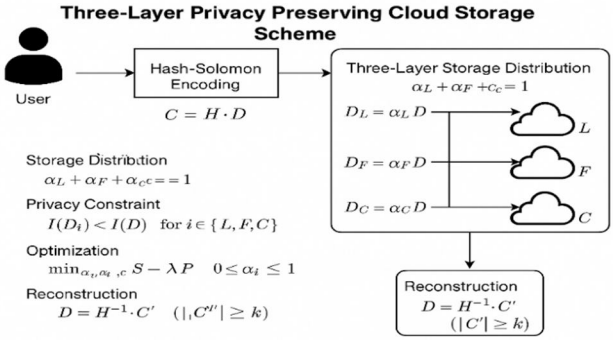


Fig. Hash-Solomon Algorithm

III. METHODOLOGY

Comprising several fog nodes, fog computing is an expanded computing architecture based on cloud computing. These nodes can process and store data to a certain extent. The proposed approach divides user data into three separate parts, each stored individually on the user's device, the fog node, and the cloud server.

A strong and clever framework for securing user data saved in cloud is introduced by the three-layer privacy-preserving cloud storage technique based on computational intelligence methodology. The need for techniques that guarantee confidentiality, integrity, and access control is urgent given the increasing dependence on cloud services for data storage. While preserving system effectiveness and user accessibility, this three-layer design seeks to protect cloud data from both internal and external attacks.

To effectively maintain and adjust security measures, the approach makes use of computational intelligence techniques including machine learning, fuzzy logic, and evolutionary algorithms.

IV. EXISTING SYSTEM

Data is usually outsourced to third-party service providers in the current cloud storage systems, which is convenient but raises serious privacy and security issues. Most of these solutions secure files prior to upload using standard encryption algorithms such as AES or RSA. Users frequently lose control over data once it has been encrypted and moved to the cloud, particularly when it comes to secure search capabilities and fine-grained access control. Effective privacy management is challenging due to these constraints, especially in collaborative and multi-user settings.

Furthermore, a lot of conventional cloud security models lack clever privacy-preserving features. They are unable to adjust to dynamic shifts in threat models, access patterns, or user behavior. Furthermore, layered security measures—which are essential for guaranteeing privacy at several levels—such as during data storage, transport, and access—are absent from the majority of current systems. Consequently, there is a higher chance of data leaks, illegal access, and attacks such side-channel or data inference.

A. Disadvantages

1) High Cost of Computation: System complexity and processing burden are increased by implementing computational intelligence techniques and overseeing three-layer security.

2) Architecture of Complex Systems: It may be challenging to administer and calls for specialized staff to design and maintain the tiered structure with AI integration.

3) Problems with Latency: Delays in user authentication and data retrieval may result from using several encryption and validation levels.

4) Cost of Initial Deployment: It takes hefty upfront infrastructure and software expenses to set up such a smart and safe cloud system.

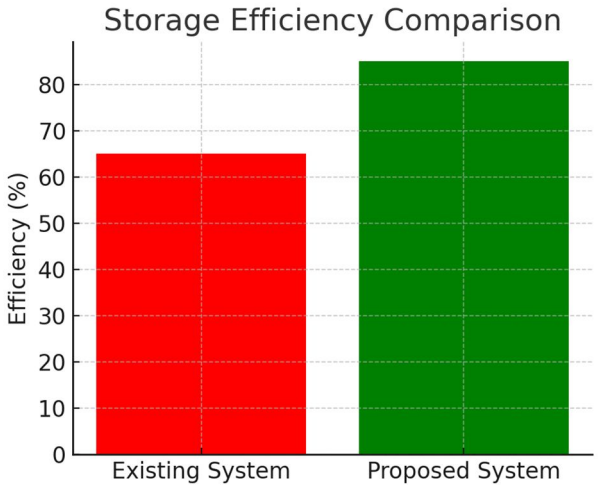


Fig. Storage efficiency comparison between the existing and proposed systems.

V. PROPOSED SYSTEM

The proposed approach introduces a three-layer storage architecture that makes use of fog computing to enhance both data security and storage efficiency. In contrast to traditional methods that place everything solely in the cloud, this design smartly spreads data across three layers—local devices, fog nodes, and remote cloud servers.

At the heart of this system lies the Hash-Solomon coding mechanism**,** which splits user data into multiple fragments. A carefully chosen portion of these fragments is retained at the local machine and fog server, while the rest is sent to the cloud. This division ensures that no single storage point contains enough information to reconstruct the original data, thereby protecting user privacy even if one layer is compromised.

A. Advantages

1) Improved Privacy of Data: The three-layer method provides robust security against unwanted access by ensuring that private information is segregated, anonymised, and encrypted.

2) Controlling Access Intelligently: The system can intelligently identify unusual access patterns and stop data breaches by utilizing computational intelligence techniques like machine learning and fuzzy logic.

3) Enhanced Effectiveness of Storage: By managing and dividing data across several levels, redundant or superfluous storage is decreased and cloud resources may be used effectively.

4) Adaptive Security Systems: Strong defence even against changing cyber-attacks is provided by the system's ability to learn from new threats and constantly update its security policies.

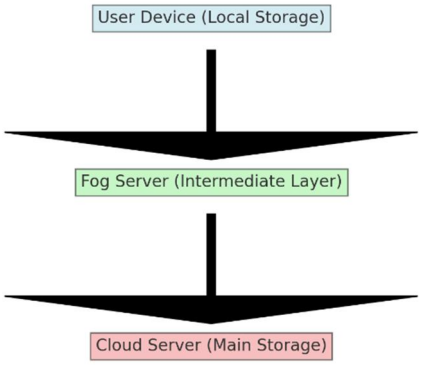


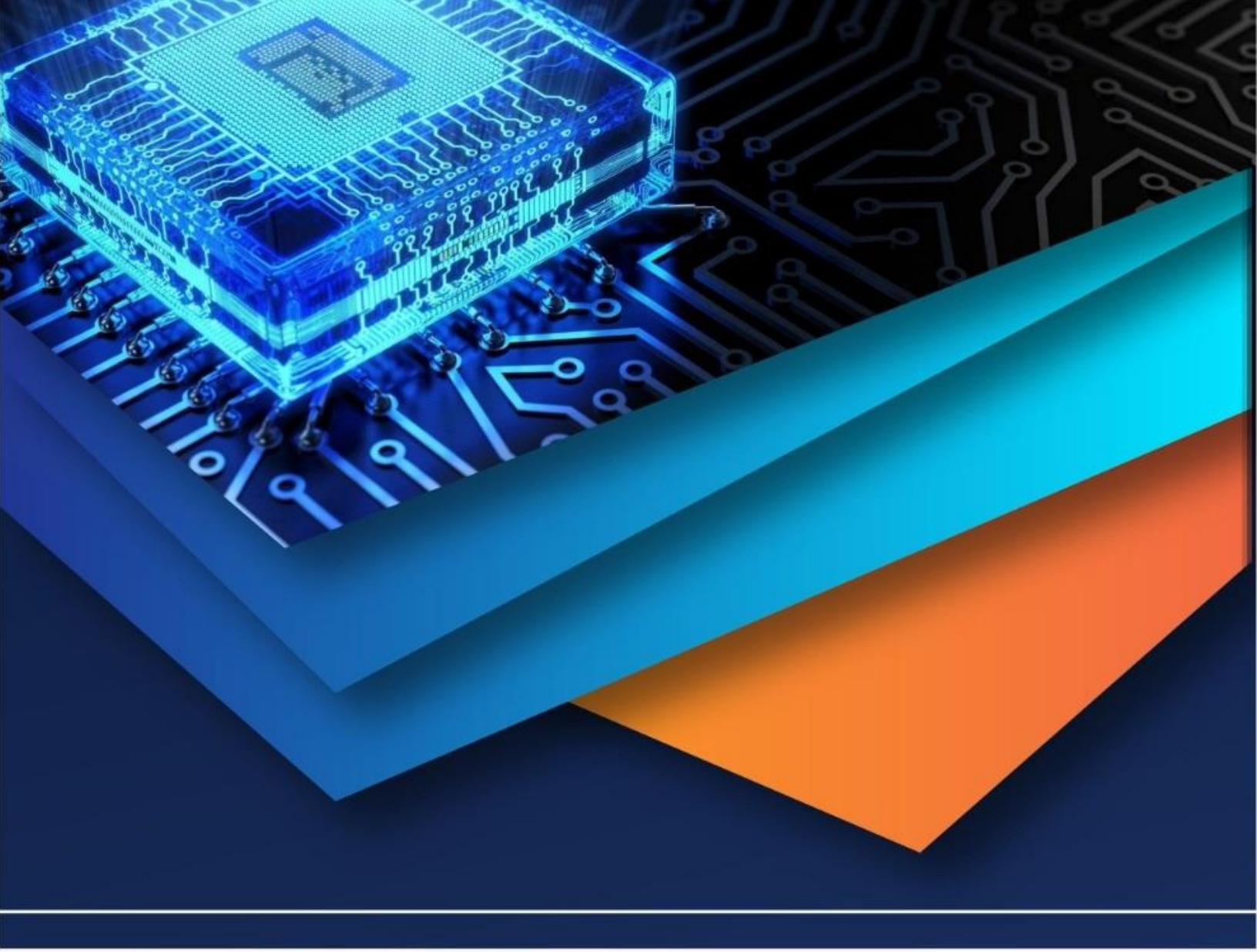
Fig. A simple three-layer storage architecture (Local → Fog → Cloud).

VI. CONCLUSION

The development of cloud computing brings us a lot of benefits. Cloud storage is a convenient technology which helps users to expand their storage capacity. However, cloud storage also causes a series of secure problems. When using cloud storage, users do not actually control the physical storage of their data and it results in the separation of ownership and management of data. In order to solve the problem of privacy protection in cloud storage, we propose a TLS framework based on fog computing model and design a Hash-Solomon algorithm. Through the theoretical safety analysis, the scheme is proved to be feasible. By allocating the ratio of data blocks stored in different servers reasonably, we can ensure the privacy of data in each server. On another hand, cracking the encoding matrix is impossible theoretically. Besides, using hash transformation can protect the fragmentary information. Through the experiment test, this scheme can efficiently complete encoding and decoding without influence of the cloud storage efficiency. Furthermore, we design a reasonable comprehensive efficiency index, in order to achieve the maximum efficiency, and we also find that the Cauchy matrix is more efficient in coding process.

REFERENCES

[1] P. Mell and T. Grance, “The NIST definition of cloud computing,” Nat. Inst. Stand. Technol., vol. 53, no. 6, pp. 50–50, 2009.
[2] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, “A survey of mobile cloud computing: Architecture, applications, and approaches,” Wireless Commun. Mobile Comput., vol. 13, no. 18, pp. 1587–1611, 2013.
[3] J. Chase, R. Kaewpuang, W. Yonggang, and D. Niyato, “Joint virtual machine and bandwidth allocation in software defined network (sdn) and cloud computing environments,” in Proc. IEEE Int. Conf. Commun., 2014, pp. 2969–2974.
[4] H. Li, W. Sun, F. Li, and B. Wang, “Secure and privacy-preserving data storage service in public cloud,” J. Comput. Res. Develop., vol. 51, no. 7, pp. 1397–1409, 2014.
[5] Y. Li, T. Wang, G. Wang, J. Liang, and H. Chen, “Efficient data collection in sensor-cloud system with multiple mobile sinks,” in Proc. Adv. Serv. Comput., 10th Asia-Pac. Serv. Comput. Conf., 2016, pp. 130–143.
[6] L. Xiao, Q. Li, and J. Liu, “Survey on secure cloud storage,” J. Data Acquis. Process., vol. 31, no. 3, pp. 464–472, 2016.
[7] R. J. McEliece and D. V. Sarwate, “On sharing secrets and reed-solomon codes,” Commun. ACM, vol. 24, no. 9, pp. 583–584, 1981.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY