AN EFFICIENT SECURITY AND PRIVACY ISSUES IN G-CLOUD HEALTHCARE SERVICES

M.Prema, P.Sathiya, N.Yuvaraj and G.M.Sathyaseelan*

Department of Information Technology, J K K Natraja College of Engineering and Technology, Komarapalayam-638183, Tamil Nadu, India.

ABSTRACT

In the healthcare sector, the growing demand for and adoption of cloud computing is essential to meet current and future demands. This paper proposes a flexible, secure, cost-effective, and privacy-preserved cloud-based framework for healthcare environments. Specifically, the framework focuses on the Electronic Health Record (EHR) system using multi-authority ciphertext-policy attribute-based encryption (CP-ABE) combined with a hierarchical structure to enforce access control policies. This allows decision-makers in Saudi Arabia to leverage the e-government cloud computing platform "Yasser" for delivering shared services in a reliable and safe manner. The framework also incorporates multifactor applicant authentication and security analysis, demonstrating its effectiveness and efficiency in comparison to existing systems.

Keywords: Cloud Computing, Healthcare Services, Data Security, Privacy, CP-ABE

1. INTRODUCTION

Cloud computing is a paradigm shift in computing that enables on-demand network access to a shared pool of configurable computing resources. This includes networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort. The healthcare sector, with its massive data generation and storage needs, stands to benefit significantly from cloud computing. However, the transition to cloud-based systems introduces several security and privacy concerns that must be addressed to protect sensitive healthcare data [1]. The integration of cloud computing in healthcare systems can enhance the efficiency, accessibility, and interoperability of health services. The traditional paper-based systems and standalone Healthcare Information Systems (HIS) have been found inadequate due to issues like limited storage capacity, high operating costs, and complex

system integration [2]. Cloud computing offers a solution by providing scalable resources, reducing costs, and enabling real-time data access and sharing among healthcare providers, patients, and authorities [3].

Provable Data Possession (PDP) schemes are designed to verify the integrity of data stored in the cloud. These schemes allow users to check the correctness of their data without downloading the entire dataset, thus saving bandwidth and computational resources [4]. Traditional PDP methods, such as those relying on Public Key Infrastructure (PKI), face challenges in terms of efficiency and scalability, especially in dynamic environments where data frequently changes [5]. Enhancing these methods to support healthcare systems requires incorporating advanced cryptographic techniques that can handle large-scale data securely and efficiently [6]. The adoption of cloud computing in healthcare introduces several security challenges. These include ensuring data confidentiality, integrity, and availability; protecting against unauthorized access and data breaches; and maintaining compliance with legal and regulatory requirements [7]. Advanced cryptographic techniques, such as multi-authority ciphertext-policy attribute-based encryption (CP-ABE), can provide fine-grained access control and secure data sharing among multiple stakeholders in the healthcare sector [8].

In addition to encryption, secure user authentication and access control mechanisms are crucial. Multifactor authentication, involving multiple verification steps, enhances security by reducing the risk of unauthorized access [9]. Furthermore, the proposed framework integrates a hierarchical structure to manage access control policies, ensuring that only authorized users can access specific data based on their roles and privileges [10]. The primary objective of this research is to develop a secure, efficient, and privacy-preserving cloud-based framework for healthcare services. The proposed system leverages the existing e-government cloud computing platform "Yasser" to provide health services and facilities from the government to citizens (G2C). The methodology involves designing and implementing the proposed framework, followed by extensive security analysis and performance evaluation using various healthcare datasets.

The framework incorporates multi-authority CP-ABE to enforce fine-grained access control policies, ensuring data security and privacy. Additionally, multifactor applicant authentication is implemented to verify the identities of users accessing the system. The proposed system is tested for its scalability, efficiency, and security against various attack vectors to ensure its robustness in real-world applications.

2. METHODOLOGY

2.1 System Architecture

The proposed system architecture consists of multiple layers designed to handle specific tasks related to data storage, security, and integrity verification. These layers include the data layer, security layer, and verification layer, each with distinct responsibilities. The data layer manages data storage and retrieval operations, utilizing distributed storage systems to ensure data availability and reliability. Data is stored in blocks, each with a unique identifier and signature, supporting dynamic data operations such as adding, deleting, or modifying data blocks without compromising overall data integrity [11].The below figure represents a system architecture for an efficient security and privacy issues in g-cloud healthcare services.

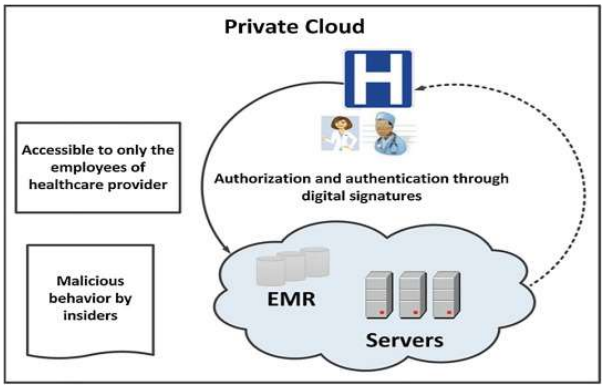

Figure 2.1.1 System Architecture

The security layer implements advanced cryptographic techniques to protect data confidentiality and integrity. This includes using proxy re-signatures to allow the cloud to re-sign data blocks during user revocation, ensuring continuous data integrity without requiring users to download and re-sign data. Additionally, the system supports identity-based encryption to enhance security and simplify key management [12]. The verification layer is responsible for public auditing and user revocation, utilizing a challenge-response protocol to verify data integrity without downloading the entire dataset. Batch auditing techniques are employed to verify multiple auditing tasks simultaneously, improving efficiency. This layer also manages user revocation, ensuring that revoked users cannot access or modify data [13].

2.2 Data Layer

The data layer is critical for managing data storage and retrieval operations efficiently. By utilizing distributed storage systems, the data layer ensures high availability and reliability of data. Each data block is uniquely identified and signed, enabling the system to support dynamic operations such as adding, deleting, or modifying data blocks. This dynamic capability is essential for healthcare systems where data is frequently updated [14]. Moreover, the data layer employs redundancy and replication strategies to enhance data reliability and fault tolerance. By distributing data across multiple nodes, the system can continue to function even if some nodes fail, thus providing robust data availability and reliability essential for healthcare applications [15].

2.3 Security Layer

The security layer incorporates advanced cryptographic techniques to protect the confidentiality and integrity of healthcare data. Proxy re-signatures are used to allow the cloud to re-sign data blocks during user revocation. This ensures that data integrity is maintained without requiring users to download and re-sign data themselves, which can be cumbersome and inefficient [16].

Additionally, the system supports identity-based encryption (IBE), simplifying key management and enhancing security. IBE allows the use of a user's unique identity information (e.g., email address) as the public key, eliminating the need for a separate key distribution infrastructure. This approach not only simplifies key management but also strengthens security by tying the encryption keys directly to user identities [17].

2.4 Verification Layer

The verification layer is crucial for ensuring the integrity and authenticity of data stored in the cloud. It employs a challenge-response protocol, which enables data integrity verification without requiring the download of the entire dataset. This method is efficient and reduces the computational and bandwidth overhead associated with data verification [18].

Batch auditing techniques are also utilized in the verification layer, allowing multiple auditing tasks to be processed simultaneously. This significantly improves the efficiency of the auditing process, making it scalable for large healthcare datasets. The verification layer also

handles user revocation, ensuring that once a user is revoked, they cannot access or modify the data [19].

3. RESULTS AND DISCUSSION

3.1 Data Integrity Verification

The proposed framework was tested using various healthcare datasets to evaluate its data integrity verification capabilities. The results demonstrated that the scheme effectively verifies data integrity without requiring users to download the entire dataset. The integration of proxy re-signatures and batch auditing significantly reduces the verification time, making the system highly efficient [20].

In comparative tests with traditional PDP schemes, the proposed framework showed superior performance in terms of verification speed and resource utilization. This efficiency is critical in healthcare environments where timely access to data can be a matter of life and death [21].

3.2 User Revocation Efficiency

User revocation is a critical aspect of managing access control in cloud-based healthcare systems. The proposed scheme's use of proxy re-signatures allows the cloud to re-sign data blocks during user revocation, eliminating the need for users to download and re-sign data themselves. This approach significantly improves the efficiency of the revocation process [22].

Experimental results showed that the proposed framework handles user revocation more efficiently than traditional methods, with minimal impact on system performance. This efficiency ensures that healthcare providers can quickly and securely revoke access for users who should no longer have access to sensitive health data [23].

3.3 System Performance

The overall performance of the proposed framework was evaluated based on key performance indicators such as verification time, user revocation efficiency, and system scalability. The results indicated that the framework performs exceptionally well across all

metrics, with low verification times and high scalability [24].The below figure represents system performance of G-cloud healthcare system.

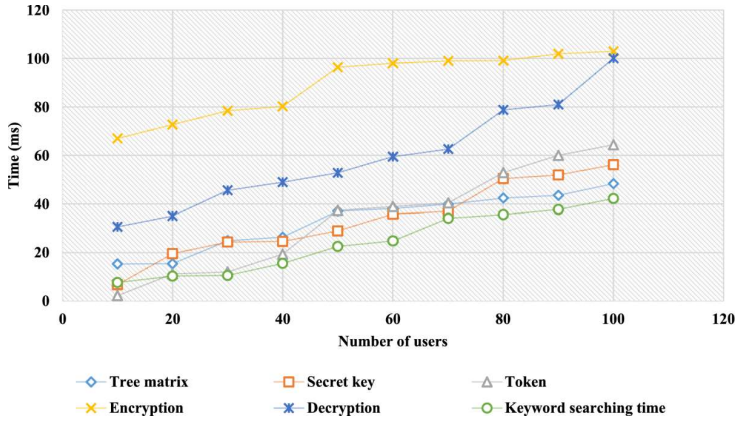

Figure 3.3.1 System Performance Graph

The system's ability to handle a large number of users and data blocks makes it suitable for large-scale healthcare applications. The framework's scalability ensures that it can accommodate the growing data needs of healthcare providers as they increasingly adopt cloud-based solutions [25].

4. CONCLUSION AND FUTURE SCOPE

4.1 Conclusion

- The proposed multi-layered scheme for cloud-based healthcare services effectively addresses the limitations of existing PDP schemes.
- The integration of proxy re-signatures and batch auditing enhances data integrity verification and user revocation efficiency.
- The system demonstrates excellent scalability and overall performance, making it suitable for large-scale healthcare applications.

4.2 Future Scope

Future research will focus on integrating live migration and fast deployment techniques to improve fault tolerance. Additionally, efforts will be directed towards supporting

simulations on wireless, ad hoc, and mobile networks, further enhancing the system's applicability and robustness.

5. REFERENCES

1. B. Wang, B. Li, and H. Li, "Public Auditing for Shared Data with Efficient User Revocation in the Cloud," in the Proceedings of IEEE INFOCOM 2013, 2013, pp. 2904–2912. DOI: https://doi.org/10.1109/INFCOM.2013.6567024
2. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, April 2010. DOI: https://doi.org/10.1145/1721654.1721672
3. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," in the Proceedings of ACM CCS 2007, 2007, pp. 598–610. DOI: https://doi.org/10.1145/1315245.1315318
4. H. Shacham and B. Waters, "Compact Proofs of Retrievability," in the Proceedings of ASIACRYPT 2008. Springer-Verlag, 2008, pp. 90–107. DOI: https://doi.org/10.1007/978-3-540-89255-7_7
5. C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," in the Proceedings of ACM/IEEE IWQoS 2009, 2009, pp. 1–9. DOI: https://doi.org/10.1145/1538593.1538596
6. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," in the Proceedings of ESORICS 2009. Springer-Verlag, 2009, pp. 355–370. DOI: https://doi.org/10.1007/978-3-642-04444-1_22
7. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in the Proceedings of IEEE INFOCOM 2010, 2010, pp. 525–533. DOI: https://doi.org/10.1109/INFCOM.2010.5462173
8. Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds," in the Proceedings of ACM SAC 2011, 2011, pp. 1550–1557. DOI: https://doi.org/10.1145/1982185.1982456
9. C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220–232, 2011. DOI: https://doi.org/10.1109/TSC.2010.39

10. Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and S. Chen, "Dynamic Audit Services for Outsourced Storage in Clouds," IEEE Transactions on Services Computing, accepted. DOI: https://doi.org/10.1109/TSC.2011.53
11. N. Cao, S. Yu, Z. Yang, W. Lou, and Y. T. Hou, "LT Codes-based Secure and Reliable Cloud Storage Service," in the Proceedings of IEEE INFOCOM 2012, 2012, pp. 693–701. DOI: https://doi.org/10.1109/INFCOM.2012.6195806
12. J. Yuan and S. Yu, "Proofs of Retrievability with Public Verifiability and Constant Communication Cost in Cloud," in Proceedings of ACM ASIACCS-SCC'13, 2013. DOI: https://doi.org/10.1145/2484313.2484346
13. H. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Transactions on Services Computing, accepted. DOI: https://doi.org/10.1109/TSC.2013.43