International Journal of Engineering Research and Sustainable Technologies
Volume 3, No.1, March 2025, P 39 - 44
ISSN: 2584-1394 (Online version)

SECURIG HEALTHCARE DATA IN THE CLOUD AGAINST INFERENCE ATTACKS

[1]G. Vishnupriya, [2] Adishwar A , [3]Chandru S, [4] Dinesh S
[1]Assistant Professor, [2,,3,4,5] UG Scholar
[1,2,3,4,5]Department of CSE, Easwari Engineering College of Technology, India
*** Corresponding author email address**: vishnupriya.g@eec.srmrmp.edu.in

DOI: https://doi.org/10.63458/ijerst.v3i1.107 | **ARK: https://n2t.net/ark:/61909/IJERST.v3i1.107**

Abstract

The E-HealthCare cloud system demonstrates important possibilities for improving healthcare quality and the well-being of people. However, it has not spread, especially due to the most important concerns about security and privacy. Existing methods for storage rely on basic access control models and are susceptible to inference attacks. In this article, we have set up an inference attack for attacks on e-HealthCare cloud systems that use fine-tuned access controls. We propose a new approach using a two-layer encryption scheme that allows for secure and effective data manipulation. The first encryption layer contains marked access guidelines. This can be tailored to any data attribute where fine access control is achieved and encryption efforts are reduced simultaneously. As a rule, role attributes and access guidelines are hidden within a second encryption layer to protect privacy. The cloud is permitted to perform a variety of mathematically intensive tasks on behalf of the user without disclosing private data, in order to use the computing power of the cloud without affecting the confidentiality of the sensitive information. To achieve this, we develop a blind data access protocol using Paillier encryption. The results of comprehensive security analysis and performance assessments confirm that the proposed solution is as efficient and efficient as a secure cloud management system.

Keywords: e-HealthCare cloud, electronic medical records (EHR), inference attacks, detailed access management, dual-layer encryption, hidden data access, access patterns confidentiality.

1. Introduction

The e-healthcare cloud system offers a solution that can transform healthcare quality and availability. Nevertheless, security and privacy concerns are still a significant challenge, especially for sensitive EHR protection. Existing solutions use a simple access control model that is both vulnerable to inference attacks like and can allow unauthorized access to non-logical access patterns.

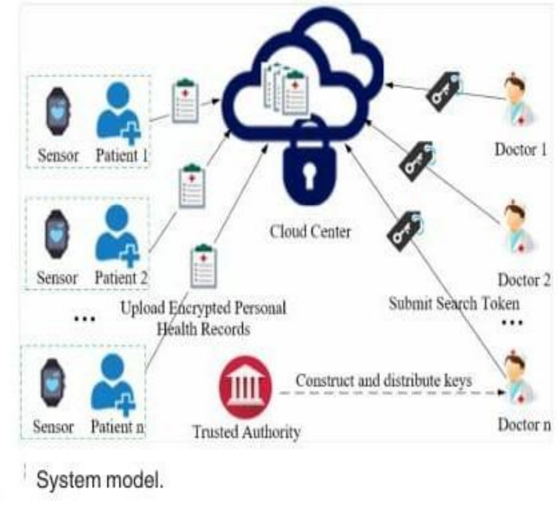

Fig 1. Securing Healthcare Data

.

This project uses two-layered augmented degradation algorithms to set up a robust e-Healthcare cloud framework that improves fine-grained access control technology. Each data attribute is subject to an encryption process that implements specific access guidelines to ensure accurate control while simultaneously improving encryption efficiency. Additionally, additional security levels are applied to role attributes and access guidelines to mitigate the risk of inference attacks figure 1. Data Protection Presentation with Paillier Encryption Presentation Data Access Protocol is also included to cover access patterns. The system provides a powerful, efficient and secure framework for accessing electronic health data (Honor) in a cloud environment by delegating computing tasks via cloud computing functions.

2. Literature Survey

Y. Miao et al. have designed an efficient revocation– based keyword search scheme capable of being controlled over time in mobile e-health cloud. By design, this enables flexible data access, whilst also protecting privacy. Wang et al. presented a secure FE keyword search batch and fine-grained encrypted for EC. Their research aims to improve access control and search time without compromising the security of data.

J. Sun and colleagues have set up a system of bilateral fine-grain access control that ensures privacy in cloud-based industrial IoT healthcare. The framework helps protect data exchange and maintain strict protection against data protection. K. Mahmood et al. established a low-cost and secure authenticated system with cloud support for distant wearable health monitoring systems, achieving security and reliability of data transmission.

J. Wang et al. It improves both data integrity (CR) and user access management (CAC) with a secure, updated framework for access control for the storage of electronic health records (EHRs) in cloud computing.

W. Zhang et al. We have developed a subtle e-healthcare cloud system that protects interference attacks, is treated unauthorizedly, and maintains flexible data access at the same time. A. U. R. Butt et al. Create role-based access control models for demands that use trust mechanisms in e-Health's cloud environments to increase security and regulate dynamic access to system resources.

Y. Bao et al. We have developed an efficient, lightweight, fine-grained, searchable data exchange scheme to maintain targeted data guidelines for secure data use in IoT-oriented and cloud-assisted smart healthcare systems. A. Ullah et al Leaded reviews of secure healthcare through Internet of Things (IoT) data aggregation and transfer. There, there were various security mechanisms associated with healthcare applications. Designed, safe-based cloud storage system for encrypted, patient oriented medical records..

R. Anitha and S. Mukherjee addressed the challenges and issues associated with ensuring sensitive health information in cloud-based health care.Lan Zhou et al. designed a secure role-based cloud storage system for encrypted patient-centric health records. Lan Zhou and colleagues have developed a cloud-secured, role-based storage system for encrypted health records focusing on patient needs.

Fahad Saeed et al. We proposed secure health data on mechanisms for common interests based on encryption and various authentication methods. Ahmed Ibrahim et al. analyzed a cloud-enabled electronic health records sharing framework with privacy and security compliance. David R. Matos et al. We proposed a method to combine encryption and access control mechanisms to ensure electronic health records in the cloud. S. Prathima, C. Priya, an international journal of Privacy Protection and Security Management Survey in Cloud-based Electronic Health Records, innovative research in computer and communications technology.

3. System Methods

3.1 Existing System

The security features of the EHR system (Electronic Healthcare Record) are primarily based on largely on simple encryption methods and also on conventional access control models, they have several limitations. Most of the current approaches apply a strict binary access control policy, which lack flexibility in granting permissions. Also most existing systems are not secure against inference attacks, where unauthorized users are able to infer sensitive data from (access) patterns. Such limitations require the development of a more sophisticated security framework which provides better fine-grained access control, infers attack counterment, and handles data privacy while ensuring effective search and retrieval functionalities.

3.2 Proposed system

To protect this information, we recommend an e-HealthCare cloud system that resists inference attacks and incorporates fine-grained access controls to maintain the privacy, security and integrity of your electronic health records (EHR). The proposed system uses a double encryption method, a blind data retrieval protocol, and a time-controllable keyword search mechanism to protect medical data against unauthorized access. Such approach allows safely storing patient record the way that access is managed and there is efficient retrieval of patient record, while addressing a major concern such us collusion attack, keyword guessing attack, user inference attack. The architecture adopts a cryptographic approach to improve both performance and usability through secure authentication mechanisms combined with lightweight encryption models.

3.2.1 Fine-Grained Access Control

Use role-based and attribute-based access controls to restrict data access according to the user's role (such as doctors, nurses, patients). In the case of EHRS inspection, authorized users can access only the information they need, reducing the chances of unauthorized access to sensitive data.

3.2.2 The Two- Tier Cryptography Framework

Attribute Based Encryption (First-Shift Encryption): This method uses an Attribute-Based Encryption Approach (ABE) to guarantee honor.

Symmetric Encryption (Second-Layer Encryption): That encrypted data is then encrypted again using a lightweight symmetric encryption algorithm before it is stored in the cloud. Overall, it is a two-layer encryption strategy that ensures protected data even if one layer is hacked.

3.2.3 Cloud Storage and Optimize the Performance

Secure Data Storage: First, the medical records are encrypted and preserved in a distributed cloud environment in which data redundancy is ensured to provide high availability and fault tolerance.

3.2.4 Protocol for Blind Data Retrieval

The design of a blind data retrieval mechanism allows cloud servers to process user queries and not learn any sensitive information about requested electronic health records (EHRs). This foils inference attacks, in which an attacker could look for patterns of access to infer private medical information.

3.2.5 Keyword Search with Time Control Keyword Search

A novel secure keyword search protocol empowers a trusted user to query medical records in an efficient way while preventing the security risk of leaking the search query to the cloud provider end. The system also has a time controllable feature that allows access to the healthcare provider for a limited time period, thereby improving security.

3.2.6 User Revocation Mechanism

The system addresses such dynamic user roles through an efficient process of revoking users. When a doctor, nurse, or other medical personnel lose access privileges, the decryption keys are revoked immediately, so they cannot gain access again.

3.2.7 Authentication and Key Management

This method requires users to provide two factors before they can be granted (logged) access into the system. First users are asked to provide their password, then users can authenticate themselves through a biometric component (e.g., via fingerprint or facial recognition).Employs a safe key management protocol to deliver encryption keys to relevant users whilst not sharing them with third-party users.

3.2.8 Mechanisms of Attack Resistance

The system is hardened against a wide range of security vectors such as:

Inference Attacks — Withholds sensible information from unauthorized users through query examination.

Keyword Guessing Attacks – Makes sure that the attackers aren't able to leverage search queries to infer medical conditions.

Collusion Attacks – Reduces threats from more than one unauthorized user combining their partial information to gain access to restricted EHRs.

4. Implementation and Result

Our approach relies on a cloud infrastructure embedded with multi-layer encryption technologies, secure data fetching protocols, and fine-grained access management strategies. It enables privacy-preserving method of electronic health records (EHRs) storage and retrieval, however also prevents inference attacks. It constantly checks user access behavior, keyword searches, and data retrieval requests for potential security threats. This system automatically issues security alerts and enforces dynamic access restrictions to protect patient data when it detects unauthorized access attempts or abnormal query patterns figure 2.

It presents a cloud-based e-healthcare platform that is stored in electronic health files to ensure electronic health records (EHRS) and simultaneously protects inference attacks. To protect sensitive medical information, the system combines a dual-layer encryption approach, comprehensive access control, and a robust data recovery method for non-measured data. It also has time-controlled keyword search technology that gives you flexible access to authorized users. Data is securely encrypted and is only called by the responsible authorities to prevent access to others in the healthcare system.

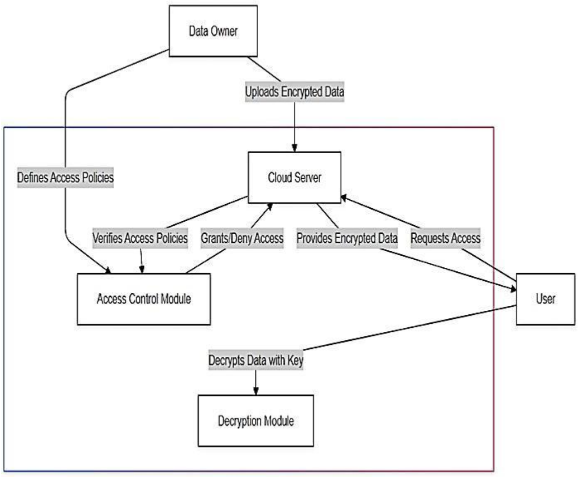

Fig 2. Architecture Diagram

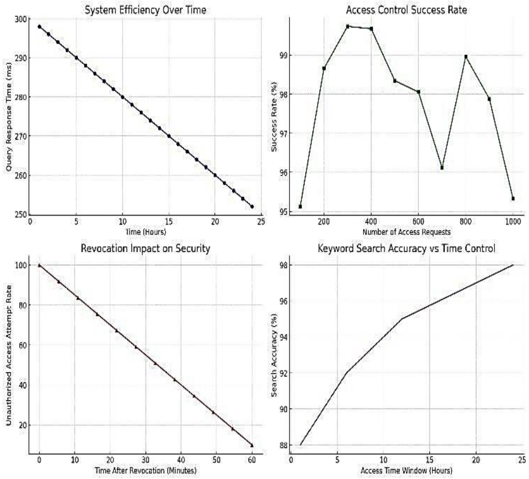

Fig 3. Analysis of Source of Helathcare Data

A cloud-based e-healthcare platform, encryption algorithms, and an access control mechanism to manage EHRs comprise the backend of this system. Data till October 2023 is in the encrypted format and stored in the cloud for secure access and storage. Using cryptographic techniques to implement the security architecture of the system, the approach preserves data privacy and defends against inference attacks to build a highly secure and efficient health care system figure 3.

This prototype figure 4. illustrates a cloud-based electronic healthcare system. In this system, electronic health files (honesty) are stored securely and carefully using encryption and careful access control methods. To protect sensitive patient data, the system works with semi-loyal data storage providers and uses a two-stage encryption strategy that uses blind data call methods.

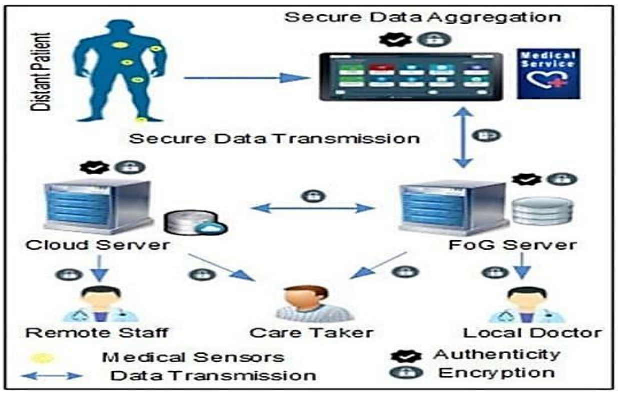

Fig 4. Prototype Models of the System

The Access Control Framework ensures secure access and processing medical records that connect your cloud platform with certified users. By using encryption techniques and keyword-controlled search functions, the system maintains both efficiency and security of data access and prevents unauthorized inference attacks on health information.

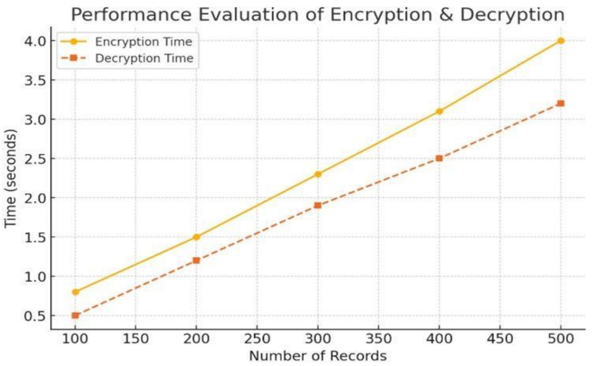

Fig 5. Performance Evaluation of Encryption and Decryption

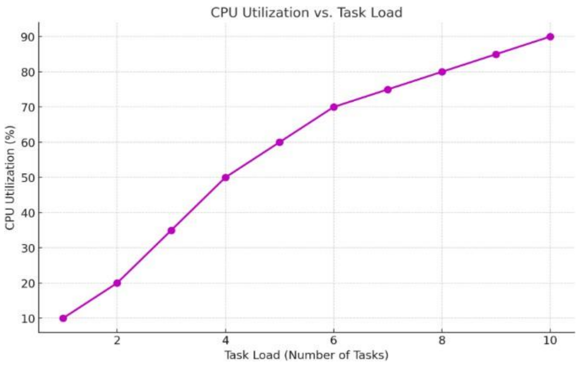

Fig 6. CPU Utilizations Vs Task Load

This system determines the basic framework for the preservation of health files and e-health care to ensure data security and electronic health files (honesty) during the storage and access phases. The system implements a double-layer encryption method in which medical documents are encrypted before they are uploaded to the cloud. If a certified person confirmed with strong login information needs access to data, the system will verify the submitted information, safely decipher the data, and ensure that sensitive information is not disclosed. Even throughout the Data AB Call process, the blind data call protocol ensures that cloud service providers are unaware of patient information. Additionally, the system can increase user cancellations and dynamically update or revoke access based on the data used by health service providers. These encryption techniques are designed to prevent data damage, so that they can provide unauthorized access to sensitive information in the event of a third party's violation.

In addition, through patient data exchange, it ensures secure monitoring input channels for healthcare professionals and patients in real-time. A blind data retrieval protocol so that the cloud service provider does not learn anything about the patient records which could be used to conduct inference attacks. In this case of user revocation, the access control mechanism effectively updates the permissions dynamically, forcing revoked users unable to retrieve any sensitive health data. By utilizing secure encryption methods and controlled search capabilities, the e-healthcare cloud system optimizes both security and usability and stands as an excellent solution in today’s healthcare data management.

Input : Encrypted EHR, User Queries, Access Requests
Output : Patient information was safely converted using detailed access control, notifications of unauthorized access, and encryption of search results before transfer.

Advantages:

This system goes beyond EHR security and assists in:

- Privacy-Preserving Management of Healthcare Data
- Access Controls for Medical Workers
- Secure Patient Record Sharing
- Some Protection from Inference Attacks
- Scalability for Extensive Healthcare Networks

The result of using this system is an e-healthcare system which is cheap, scalable wirelessly, high performance, and provides good security, to guarantee efficient use of computer resources, and patient data security and privacy in modern medical environments figure 5 and figure 6.

5. Conclusion

Creating cloud systems for e-healthcare that are resistant to inference attacks can significantly improve security by implementing encryption strategies using two layers. Detailed measurements of blind data calls protocols and access control. The new system focuses on protecting patient data protection and effectively managing health data. The proposed solution, which includes encryption methods and IoT-based security features, represents an advanced step towards future secure and scalable electronic healthcare systems that leverage existing issues related to data security and accessibility.

References

1. Y. Miao and colleagues, "Time Regulations and Efficient Revocation Methods for Mobile E-Health Cloud," IEEE Transactions on Mobile Computing, Vol. 5, pp. 3650-3665, May 2024, doi: 10.1109/tmc.2023.3277702.
2. H. Wang, J. Ning, X. Huang, G. Wei, G. S. Poh and X. Liu, "Secured, fine-grained keyword search for e-healthcare cloud", Trusted and secure computing in IEEE Transactions, Vol. 3, Pages 1307-1319,May2021,doi:10.1109/tdsc.2019.2916569.
3. J. Sun,Y.yuan,M.tang , x.cheng ,x. Nie and M. U. Aftab, "Data Protection for Cloud-Enabled IoT Healthcare - Basic Fine Control," IEEE Transactions on Industrial Informatics, Vol. 9, pp. 6483-6493, September2022,2:10.1109/TI.2021.313345
4. K. Mahmood et al. , "Cloud-supported, secure, cost-effective, authenticated solutions for remote wearable health monitoring systems," IEEE Transactions Network Science and Engineering, Vol. 5, pp. 2710-2718, September 1st. 2023. doi: 10.1109/tnse.2022.3164936
5. J. Wang, X. Yin, J. Ning, S. Xu, G. Xu and X. Huang, "Cloud-based Secure and Updated Access Control for EHRS", IEEE Transactions on Services Computing, Vol. 4, pp. 2939-2953, July and August. 2023, doi: 10.1109/tsc.2022.3232 230.
6. W. Zhang, Y. Lin, J. Wu and T. Zhou, "e-Healthcare Cloud System. 14, no. 1, pp. 167-178, January 1st 2021, doi: 10.1109/tsc.2018.2790943.
7. U. R. Butt et al. , "Improved Role-Based Control Approach Using Trust Mechanisms in E-Health Cloud Environments," IEEE Access, Vol. QIU and X. Cheng, "Safe and Light Thin Data Exchange in Cloud Support and IoT-Oriented Smart Healthcare Systems," IEEE Internet Journal, Vol. 9, no. 4, pp. 2513-2526, February 15th. 2022,DOI : 10.1109/Jiot.2021.3063846
8. Y. Bao, W. Qiu and X. Cheng exist in the IEEE Internet of Things Journal. 9, no. 4. 2513-2526, February 15, 2022, doi: 10.1109/jiot.2021.3063846.
9. Jhanjhi, "Agreement and Sending of Secure Healthcare Data to IoT", IEEE Access
10. R. Anitha, Saswati, Mukherjee, 1201-1209 : Doi : 10.1007-3-642-41674-3-3-167
11. LAN Zhou ,Vijay , Varadharajan , Kanchi ,l Gopinath, (2016). Safe-Flow-based cloud storage system for encrypted patient orientation. The Computer Journal, 59(11):1593 doi:10.1093/comjnl/bxw019
12. Fahad, Saeed, Alamri., Ki-Dong, Lee. (2015). Secure sharing of health data over cloud.1-5.doi:10.1109/NSITNSW.2015.717 6425
13. Ahmed, Ibrahim. , Baban, A., Mahmood. , Mukesh, Singhal. (2016). A safe framework for joint use of electronic health records rather than clouds. 1-8. doi:10.1109/segah.2016.7586273
14. David, R., Matos. , Miguel, L., Sparrow. , Pedro, Adam. (2018). Ensure electronic health records in the cloud. 1- doi:10.1145/3195258.3195259
15. S., Prathima. , C., Priya. (2020). Data protection agencies and security management in research cloud-based electronic health records. 21-29. doi:10.1007/978-981-15-32849_3