Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Secured and Encrypted Healthcare Records with Granular Access Control in Distributed Systems

Satish Tukaram Pokharkar [1], Dr.L.K. Vishvamitra[2], Borude Krushna Maruti[3], Suyog Sudam Medh[4]
[1] *Computer Science and Engineering department, Oriental University, Indore.*
[2] *Computer Science and Engineering department, Oriental University, Indore.*
[3] *Computer Science and Engineering department, adsul technical campus, Ahmadnagar.*
[4] *Computer Science and Engineering department, adsul technical campus, Ahmadnagar.*

ARTICLE INFO

Received: 26 Dec 2024

Revised: 14 Feb 2025

Accepted: 22 Feb 2025

ABSTRACT

Modern medical applications address complexities of earlier research, focusing on enhancing security and efficiency. The digitization of healthcare is being enhanced through information technology and computing, enabling the development of various new technolo- gies and medical devices. While existing systems have seen many more advances to save patients time and money, provide accurate care, and keep sensitive patient records secure, the biggest significant issue is confidentiality. To address the current security concerns in order to develop and construct the prototype model for security research work. For sensi- tive patient health records on database web servers. Existing efforts only data encryption can protect patient records from insider threats. The security of the physical layer of the SeSPHR Application is used in the proposed research work using keylogging techniques, the second to prevent insider attacks (external or internal attack like collusion attack, SQL injection at- tack, etc.) and store sensitive information or data of users or patients across multiple data servers using multi-instance database security (Chunks), and the third, and most importantly, implement a multiauthority search policy for encrypted data using the Access Control List (ACL) using Cipher's Attribute-based Encryption (CP-ABE In the present research work is being added to securely clearly state the format of patient data records in multiple chunks (small pieces) and to use cryptosystems because of confidentiality of a patient's medical information's. Specifically, proposed research task benefits to use the SHA hashing tech- nique each user to allow access to specific data records. This research work investigates the proposed Role Base Access Control (RBAC) and the proposed Advanced Encryption Algorithm (AES)-512 bit encryption techniques for secure data storage and sharing for end- user strategies for securing access to the data. This work uniquely integrates multi-authority searchable encryption with AES-512 with AES-512 to ensure secure and efficient healthcare data management. This work also included the implementation of a backup server strategy, which functions as an all distributed data servers use an ad hoc network data recovery for proxy storage server.

Medical information is stored in hospital databases. Diagnosis and patient informa-

Tion have been secured in medical databases. Some data in medical databases is sensitive information and access to that data should be restricted to authorized individuals. Addition- ally, data integrity must be safeguarded to prevent unauthorised individuals from attempting

Keywords: User data privacy, ABE (Attribute-Based Encryption), Paillier encryption, forward security, Multi-authority, SHA Algorithm, Hashing Functions, encrypted data search, Wireless network.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

INTRODUCTION

Medical data encompasses a wide range of information, Including patient records, Diagnoses, Treatments, and raw visual data such as EEG monitoring samples. This information is categorized into two main classifications: non-sensitive data and sensitive information, which includes patient records or data that can be linked to a patient. Sensory data, also referred to as measurement data, consists exclusively of sensor samples and is therefore classified as non-sensitive. In the context of EEG, sensory data comprises numerical values that represent voltages measured on a patient's scalp. In certain scenarios, Such as when EEG readings are stored in EDF+ format, Patient data may inadvertently be included in the data file, thereby compromising the security of the entire file. To mitigate this risk, healthcare information can be stored in a database. While the sensory data from EEG measurements is secured within such a file, Personal information is removed. Only identifiable details are retained in a medical database, which contains references to sensory data files. Metadata, which describes the actual statistics, is also included in the medical database. As previously mentioned, a medical database is a structured collection of medical data. This discussion focuses on relational databases, as opposed to other types such as XML databases. The methodologies outlined here are equally applicable to non-relational databases. A relational database consists of tables, each organized into rows and columns, forming a matrix that expands vertically as data is added. A table can be viewed as a collection of data items. The dimensions, objectives, and applications of medical databases exhibit some variation. These range from compact databases maintained by hospital departments that record diagnoses to extensive national medical record systems, encompassing a wide spectrum of data management. Numerous databases contain patient information, including identifiers such as the patient's name. Frequently, these databases utilize anonym zed data solely for statistical analysis or research purposes. MeDIA is capable of storing sensory data, including EEG, MRI, and CT scans. In addition, it encompasses related patient health information and annotations, which serve as examples of metadata. The primary benefits of MeDIA over the mere storage of binary data include its capacity to manage descendants, accommodate unpredictability, and facilitate refactoring, as well as its ability to integrate diverse data types such as EEG and MRI. Furthermore, if a user wishes to access both EEG and MRI data for a specific patient, she can utilize MeDIA rather than querying multiple databases individually. MeDIA distinguishes itself from conventional electronic medical record systems in three key aspects.

OBJECTIVES

- To develop a secure authentication protocol for physical layer security in SeSPHR Application.
- To implement Access Control List (ACL) using Cipher Text - Policy Attribute Based Encryption (CP-ABE) access policy methodology preserves the confidentiality of the PHRs by restricting the unauthorized users.
- To design an approach for preservation of insider attacks using multi-instance (Chunks) database security for securely distributing the confidential data in multiple data in- stances for employing the Secret Shamir Hashing algorithm.
- To perform statistical analysis on the confidential data without compromising its pri- vacy and to provide highest security from any type external or internal attack like collusion attack, SQL injection attack, etc.
- Performance analysis of the proposed approach in secure healthcare database and research work explores secure data storage and sharing using the proposed AES 512 encryption algorithm and Role Base Access Control (RBAC) for a secure data access scheme for the end user.

METHODS

- **Keylogging:**

Front-end security is the most crucial module in our research work. Therefore, keylog- ging technology is employed in healthcare apps for frontend security concerns. This Keylogging method is used to prevent phishing attempts on password security appli- cations. Consequently, healthcare applications are safer. Key-logging, also known as keyboard capture is the practice of secretly recording each key pressed on a keyboard such that no one using the keyboard is aware that their actions are being watched.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Figure 1.3: Keylogging Technique

In this research, the keylogging approach is employed to defend against keylogging attacks and enhance the security of our application's login page or front end. It will employ a calculator keypad script to set the password at registration and login time, disguise the password as a unique combination of random numbers, and provide access through OTP and keystroke events.

Access Policy:

The suggested system gives that user who is a component of the system access. The varied searching capabilities for distinct keywords that are encrypted with access poli- cies of different user searching abilities are provided by attribute- or aspect-based en- cryption. The proposed work offers a variety of criteria for access policies for distinct users, along with search capabilities and an approved access key.

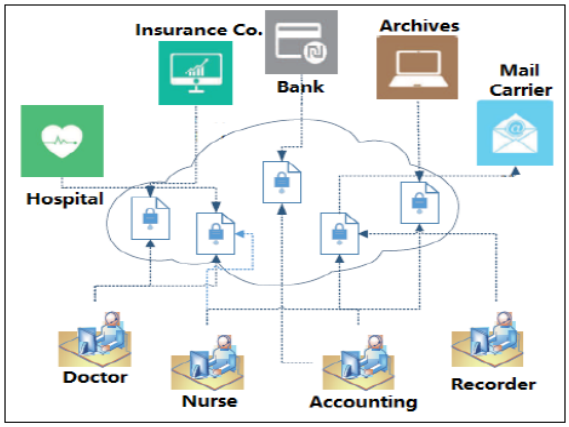

Figure 1.4: Access Policies

The proposed system grants access to users who are part of the system. It offers diverse search functionalities for various keywords, which are secured through access policies tailored to the different searching capabilities of users. The work presented introduces multiple criteria for access policies applicable to distinct users, in addition to search functionalities and an authorized access key.

Multi-authority

This study validates the capability to query all data entries that have been stored in a database in multiple segments. The primary objective of this initiative is to locate content that was encrypted at the time of upload. In a multi-authority database [1], it indicates that all authorities can grant users and clients associated with various authorities' access to its search functionality. The search capability is further improved through the implementation of an aspect-based encryption technique.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

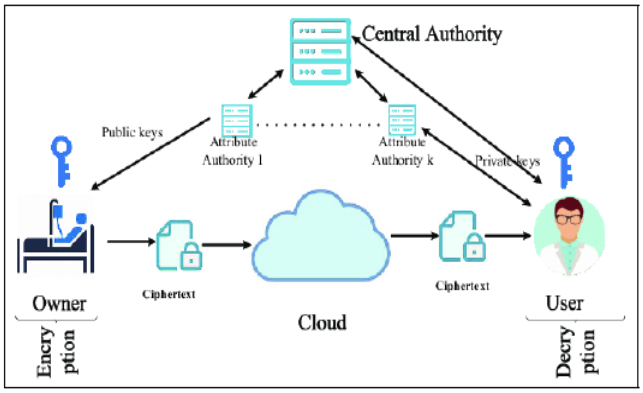

Figure 1.5: Multi-Authority

RESULTS

Figure 6.22 & 6.23 from the second experiment illustrates the effectiveness of data encryption by demonstrating how quickly it can encrypt data. Based on the provided chart, here summarize the performance of the algorithms across various file sizes. AES encryption generally demonstrates the best performance, with the lowest encryption times for each file size (50 KB, 100 KB, 200 KB, 500 KB, 800 KB, 1024 KB (1MB), 1500 KB, and 2048 KB (2MB)) and consistently fast decryption times. In contrast, the SHA-512 encryption times are consistently higher, making SHA-512 inefficient for direct data encryption in terms of performance. InnoCipher exhibits encryption times better than AES & SHA, but it shows performance that makes it good in decryption with similar performance as AES & SHA. Therefore, from the graph, AES encryption appears to offer the best balance of speed and efficiency for encryption and decryption, while the proposed InnoCipher provides a better choice. InnoCipher would likely be a good option for integrity checks or hashing.

Optimized Decryption Speed: InnoCipher achieves decryption performance comparable to AES, which is known for its fast decryption, but is higher on the scale of SHA-512. This makes it suitable for applications where quick access to the decrypted data is paramount.

Lower Overhead on Small Files: For smaller file sizes (50KB - 200KB), Inno- Cipher presents itself as a superior method in speed where other algorithms can not show their power. As a result InnoCipher can be considered good to use.

Data Integrity and Encryption Coupling: By leveraging InnoCipher for en- cryption alongside AES decryption, the design will potentially achieve more than SHA-512.

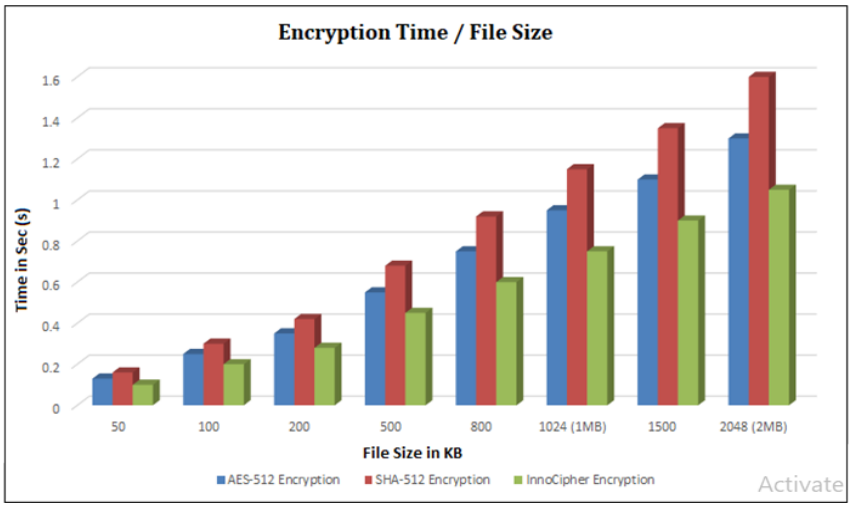

Figure 1.6: Comparison graph of encryption time with data size for all key sizes

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

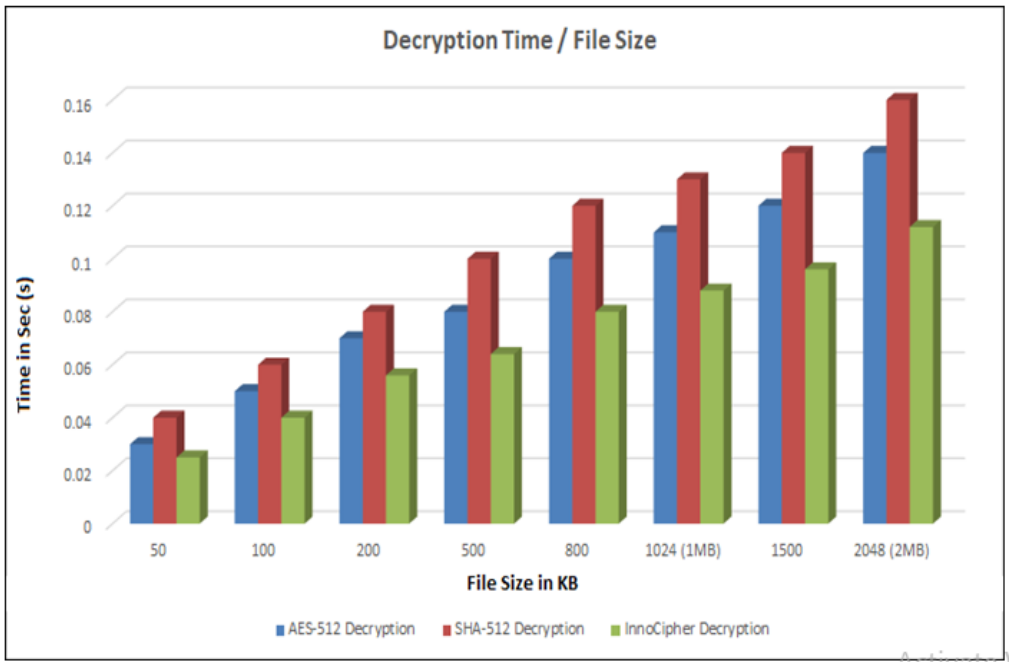

Figure 1.7: Comparison graph of decryption time with data size for all key sizes

File Size (KB)	AES En- cryption	AES De- cryption	SHA-512 Encryp- tion	SHA-512 Decryp- tion	InnoCipher Encryp- tion	InnoCipher Decryp- tion
50	0.13	0.03	0.16	0.04	0.10	0.025
100	0.25	0.05	0.30	0.06	0.20	0.040
200	0.35	0.07	0.42	0.08	0.28	0.056
500	0.55	0.08	0.68	0.10	0.45	0.064
800	0.75	0.10	0.92	0.12	0.60	0.080
1024 (1MB)	0.95	0.11	1.15	0.13	0.75	0.088
1500	1.10	0.12	1.35	0.14	0.90	0.096
2048 (2MB)	1.30	0.14	1.60	0.16	1.05	0.112

Table 1: Performance comparison of proposed algorithm with existing methods

Table 1 shows the performance comparison of the proposed (InnoCipher) algorithm with two existing methods (Method A. AES-512 and Method B. SHA-512) on two different datasets (Dataset 1 and Dataset 2). The performance of each method is mea- sured using various metrics such as accuracy, precision, recall, and F1-score. The proposed algorithm shows superior performance compared to the existing methods on both datasets.

DISCUSSION

This research addressed the critical issue of secure, authorized, and encrypted health- care record management in distributed systems by implementing a Fine-Grained Ac- cess Control (FGAC) mechanism. The research work

aimed to overcome challenges associated with data breaches, unauthorized access, and inefficient encryption techniques in healthcare environments by integrating advanced cryptographic methods and access control policies.

This research holds significant relevance to the healthcare industry in several key ways:

Data Security and Privacy: With the growing concerns about data breaches and unauthorized access to sensitive healthcare information, this research introduces a ro- bust security framework that ensures only authorized individuals can access patient records. By implementing fine-grained access control, healthcare organizations can enforce strict privacy regulations, safeguarding patient data against cyber threats.

Compliance with Regulations: Healthcare providers must comply with stringent pri- vacy laws like HIPAA (Health Insurance Portability and Accountability Act) in the

U.S. or GDPR (General Data Protection Regulation) in Europe. The encryption and access control mechanisms explored in this research can help healthcare institutions meet these legal requirements, avoiding costly fines and reputational damage. Efficient Data Sharing: In distributed healthcare systems, it is crucial for medical records to be accessible across different locations and departments while maintaining confidentiality. Fine-grained access control allows data to be shared securely among authorized entities (such as doctors, specialists, and medical institutions) without com- promising patient privacy, ensuring smooth and efficient healthcare delivery. Patient Trust and Engagement: Patients are increasingly concerned about the secu- rity of their medical records. By implementing encrypted healthcare records with clear access policies, patients can trust that their information is being handled securely. This trust encourages more active participation in their healthcare journey, leading to better outcomes. Reduction in Fraud and Misuse of Data: The fine-grained control allows for de- tailed tracking of who accessed what data and when, significantly reducing the chances of data misuse or fraud. This is especially important in preventing identity theft, in- surance fraud, and unauthorized treatment decisions based on falsified records.

REFRENCES

[1] L. Xu, S. Sun, X. Yuan, J. K. Liu, C. Zuo and C. Xu, "Enabling Authorized Encrypted Search for Multi-Authority Medical Databases," in IEEE Transactions on Emerging Topics in Computing, vol. 9, no. 1, pp. 534-546, 1 Jan.-March 2021, doi: 10.1109/TETC.2019.2905572

[2] M. H. Au, T. H. Yuen, J. K. Liu, W. Susilo, X. Huang, Y. Xiang, and Z. L. Jiang, "A general framework for secure sharing of personal health records in cloud system," Journal of Computer and System Sciences, vol. 90, pp, 46-62, 2017.

[3] A. Abbas, K. Bilal, L. Zhang, and S. U. Khan, "A cloud based health insurance plan recommendation system: A user cantered approach, "Future Generation Computer Systems, vols. 4344, pp. 99-109, 2015.

[4] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Transactions on Parallel and Distributed Systems, 2013, vol. 24, no. 1, pp. 131–143.

[5] J. Li, "Electronic personal health records and the question of privacy," Computers, 2013, DOI: 10.1109/MC.2013.225.

[6] T. S. Chen, C. H. Liu, T. L. Chen, C. S. Chen, J. G. Bau, and T.C. Lin, "Secure Dynamic access control scheme of PHR in cloud computing," Journal of Medical Systems, vol. 36, no. 6, pp. 4005– 4020, 2012.

[7] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," IEEE Communication Surveys and Tutorials, vol. 15, no. 2, pp. 1–17, Jul. 2012.

[8] R. Wu, G.-J. Ahn, and H. Hu, "Secure sharing of electronic health records in clouds," In 8th IEEE International Conference on Collaborative Computing: Networking, Applications and Work sharing (Collaboration), 2012, pp. 711-718.

[9] A. N. Khan, ML M. Kiah, S. A. Madani, M. Ali, and S. Shamshir band, "Incremental proxy re-encryption scheme for mobile cloud computing environment," The Journal of Supercomputing, Vol. 68, No. 2, 2014, pp. 624-651.

[10] D. C. Kaelber, A. K. Jha, D. Johnston, B. Middleton, and D. W. Bates, "A research agenda for personal health records (PHRs)," Journal of the American Medical Informatics Association, vol. 15, no. 6, 2008, pp. 729-736.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[11] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable and fine-grained data access control in cloud computing," in Proceedings of the IEEE INFOCOM, March 2010, pp. 1-9.
[12] A. Abbas and S. U. Khan, "A Review on the State-of-the-Art Privacy Preserving Approaches in E-Health Clouds," IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 4, pp. 1431-1441, 2014.
[13] M. Shamim Hossain, Ghulam Muhammad, et al." Cloud-assisted Industrial Internet of Things (IIoT) – Enabled framework for health monitoring." 2016 evier B.V.
[14] Ming Li, Shucheng Yu, and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute based Encryption", IEEE Transactions On Parallel and Distributed Systems 2012, vol. 21, no. 1, pp. 134–141, 2015.
[15] M. Vida, O. Lupse and L. Stoicu-Tivadar, "Improving the interoperability of healthcare information systems through HL7 CDA and CCD standards," 2012 7th IEEE International Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara, Romania, 2012, pp. 157-161.
[16] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, Cipher text-policy attribute-based threshold decryption with flexible delegation and revocation of user attribute 2009.
[17] Xilei Xu, Dongyuan Shi and Jian Fang, "Privacy-preserving personal health record system using attribute-based encryption,"Master'sthesis, WorcesterPolytechnicInstitute, 2009.