International Journal of Engineering Research and Science & Technology

EBMD: EFFICIENT BASED MEDICAL DATA SHARE IN DATABASE

SHANGAM GEETHA [1], TUMULURI SAI PRANITHA [2], DUNUKUNALA AKHILA [3], AYIOULU PAVAN [4], AVULA SHIVA KUMAR [5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— Cloud computing has transformed medical data storage by allowing healthcare institutions to outsource data management to external service providers. While this shift offers enhanced scalability and reduced infrastructure costs, it also introduces significant security and privacy concerns due to the storage of sensitive patient information on untrusted third-party servers. Traditional cryptographic techniques, such as searchable encryption, provide partial solutions but suffer from notable limitations, including vulnerability to leakage-based attacks, high computational overhead, and poor scalability in large-scale environments. To address these challenges, we propose EBMD, a novel outsourcing protocol that integrates an ordered additive secret sharing algorithm with a unique index permutation technique. ECMD ensures efficient and secure outsourcing of medical data while concealing both the data content and access patterns from potential adversaries. Our experimental evaluation demonstrates ECMD superior performance and scalability, with a single storage.

Index Terms – EBMD, Medical Data Sharing, Healthcare Database, Data Privacy, Electronic Health Records, Secure Data Management, Cloud Database, Interoperability, Access Control, Cryptography.

I. INTRODUCTION

The digitization in healthcare has led to the widespread use of Electronic Health Records (EHRs), which are essential for clinical diagnosis, treatment, and improving patient care. As healthcare centres generate and

manage vast amounts of data, many institutions are outsourcing medical data storage and processing to external servers and cloud services. While this approach offers numerous benefits, such as reduced costs and enhanced accessibility, it also introduces significant security and privacy concerns.

Outsourcing medical data to external servers poses several risks. Unauthorized access to sensitive information can lead to identity theft, financial fraud, and damage to the reputation of healthcare centres, illustrated in Data breaches can occur due to vulnerabilities in the external servers, insufficient security measures, or sophisticated cyber-attacks. Moreover, once data is outsourced, healthcare centres may lose some control over how it is managed and protected, increasing the risk of data exposure.

Recent years have seen a growing interest in developing secure systems for outsourcing medical data. Some approaches leverage searchable encryption techniques to enable secure medical data outsourcing while providing search capabilities. Attribute-based encryption (ABE) has been used to enforce fine-grained access control on e-healthcare clouds. Additionally, proxy re-encryption (PRE) has been employed in some works to facilitate sharing of medical data across multiple mutually distrusting domains. While these encryption-based solutions provide a high level of security, they face several critical challenges. First, the centralized nature of these solutions creates a single point of failure, jeopardizing the entire system if compromised.

Second, during storage and retrieval operations, the correspondence between encrypted data and access operations can be exposed, potentially allowing inference attacks. Although generic countermeasures like oblivious access have been proposed, they often require complex cryptographic primitives and are computationally expensive, limiting their practicality in real-world applications. Furthermore, as quantum computing advances, encrypted data stored on external servers could become vulnerable to offline brute force attacks.

II. RELATED WORK

A. Searchable encryption with autonomous path delegation function and its application in healthcare cloud

Outsourcing medical data to healthcare cloud has become a popular trend. Since medical data of patients contain sensitive personal

information, they should be encrypted before outsourcing. However, information retrieval methods based on plaintext cannot be directly applied to encrypted data. In this article, we present a new cryptographic primitive named conjunctive keyword search with secure channel free and autonomous path delegation function (AP-SCF-PECKS), which can be applied in scenarios where patients want to search for and autonomous delegate their private medical information without revealing their private key. Particularly, the proposed solution allows patients to set up multi-hop delegation path with their preferences, and the delegated doctors in the path can search for and access the patient's private medical information with priority from high to low. Patients can ensure that authorized doctors are always trustworthy, and unauthorized users cannot obtain the private medical information of patients. Moreover, the scheme supports the conjunctive keyword search, secure channel free, and is secure against chosen keyword attack, chosen ciphertext attack, and keyword guessing attack. The security of proposed scheme has been formally proved in the standard model. Finally, the performance evaluations demonstrate that the overhead of proposed scheme are modest for healthcare cloud scenarios.

B. Secure sharing of personal health records in cloud computing: Ciphertext-policy attribute-based signcryption.

The sharing of Personal Health Records (PHR) in cloud computing is a promising platform of health information exchange. However, the storage of personal medical and health information is usually outsourced to some third parties which may result in the exposure of patients' privacy to unauthorized individuals or organizations. In order to address this security loophole, we suggest a promising solution. We propose a new approach for fine-grained access control and secure sharing of sign crypted (sign-then-encrypt) data. We call our new primitive Ciphertext-Policy Attribute-Based Signcryption (CP-ABSC) which satisfies the requirements of cloud computing scenarios for PHR. CP-ABSC combines the merits of digital signature and encryption to provide confidentiality, authenticity, unforgeability, anonymity and collusion resistance. The correctness, security and efficiency of this scheme are also proven.

C. ''Secure outsourced blockchain-based medical data sharing system using proxy reencryption,

The security and privacy of electronic health records (EHRs) have received considerable

attention from healthcare workers and researchers. To ensure security, various encryption and decryption schemes as well as key management protocols have been developed. However, owing to sharing and scalability issues, additional security technologies have been proposed. Nonetheless, these technologies cause other problems, such as efficiency issues. Blockchain-based EHR management systems have been proposed to overcome computational overhead. However, because most blockchain systems are installed by outsourcing companies, EHRs may be leaked to the company. Hence, we herein propose a blockchain-based EHR management scheme with proxy re-encryption. In this scheme, we set a proxy server that re-encrypts the ciphertext between file servers, thereby solving EHR sharing issues. Furthermore, because the server is separated from the blockchain system, the outsourcing company cannot manipulate the server or access the records. In addition, the blockchain assists in access control by using smart contracts, thereby enabling secure and efficient EHR sharing. By performing security analysis, we prove that our proposed scheme solves the aforementioned security problems. In addition, we experimentally demonstrate the efficient operation of the proposed system.

III. PROPOSED METHODOLOGY

Maintained via secret sharing (no full data exposed at any point). Strong (conceals access patterns via index). An intuitive way to protect the medical data record is to encrypt the value and outsource the ciphertext. However, this approach suffers from the risk of offline brute force attacks, where adversaries can attempt to decrypt the ciphertext by trying all possible keys. To mitigate this risk, we propose to combine encryption with secret sharing, which divides the encrypted data into multiple shares and distributes them among server.

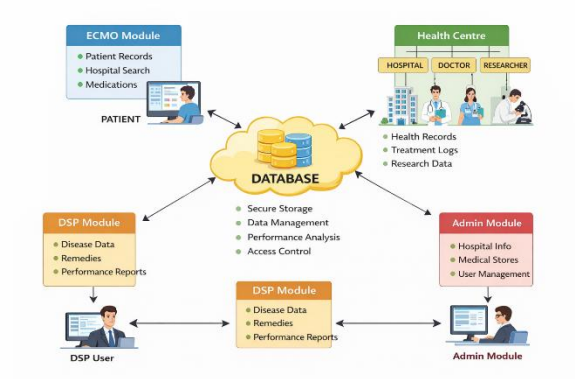


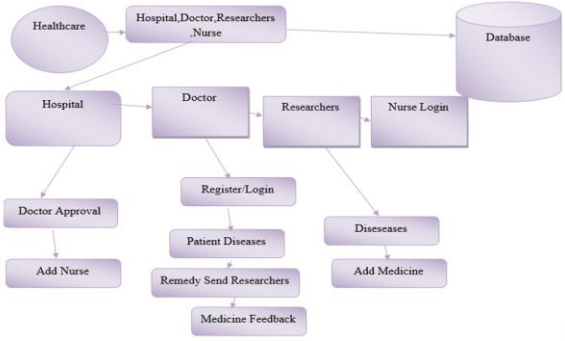
Fig. 1: System Overview

1. Health Centre

The healthcare management system consists of four main roles: hospital, doctor, nurse, and researcher. The hospital acts as the central authority that maintains a register and controls user authentication through a user ID and password. Doctors must first register in

the doctor module, but they can only log in after receiving hospital consent and approval. This approval process ensures that only verified physicians can access patient data and provide treatment. Nurses are added by the hospital and support doctors by updating patient records and assisting in treatment activities.

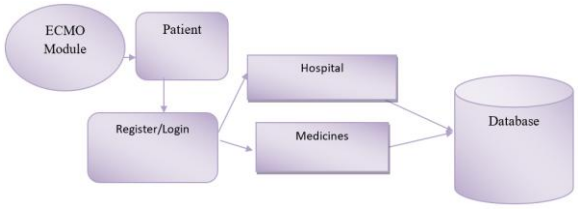
Once approved, the physician treats sick patients, prescribes medications, and shares treatment details with researchers. Researchers also register and log in using secure credentials. They analyze the medications and provide feedback or suggestions to the physician. Sometimes, researchers may have disagreements based on different medical opinions. Through controlled collaboration among all roles, the system ensures secure access, proper approvals, and effective coordination in patient care and medical research.



2. ECMO Module

The ECMO module is designed to manage and store critical patient information in a secure and organized manner. Each patient is required to complete a registration process in which personal details, medical history, and emergency information are recorded in the system. After successful registration, the patient is provided with a unique user ID and password to access the ECMO module. Through this secure login, the patient can view their profile, update basic details, and monitor treatment-related information.

Once logged in, the patient searches for a suitable hospital that provides ECMO facilities and specialized care. The system allows patients to view hospital details, availability, and contact information to make informed decisions. After consultation with a physician, the patient receives prescribed medication as part of the treatment process. All prescribed drugs and treatment updates are recorded in the ECMO module, ensuring continuity of care, accurate documentation, and secure access to critical patient data throughout the treatment journey.

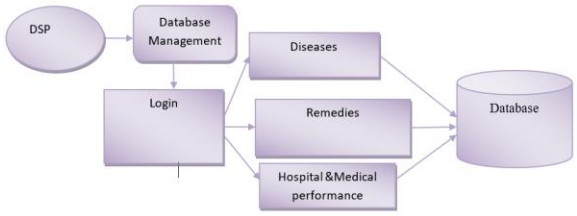


3. Database Service Provider

The DSP module is designed to provide secure access and organized management of clinical and performance-related data. Each DSP user logs into the system using a unique user ID and password, ensuring that only authorized personnel can access sensitive medical information. After authentication, the DSP can view and manage detailed records related to patient diseases, which helps in understanding illness patterns and treatment requirements.

The module also maintains a structured database of remedies, including medications, therapies, and recommended treatment protocols. This information supports accurate decision-making and improves the quality of patient care. In addition, the DSP monitors hospital performance by analysing indicators such as patient recovery rates, service efficiency, and resource utilization. Medical performance data, including physician effectiveness and treatment outcomes, are also recorded and evaluated.

By integrating disease data, remedies, hospital performance, and medical performance in a single platform, the DSP module supports clinical analysis, quality improvement, and evidence-based healthcare management.

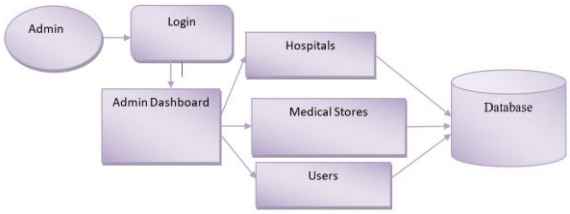


4. Admin

The admin module plays a central role in managing and controlling the entire healthcare system. The admin logs into the system using a secure user ID and password, ensuring that only authorized administrators can access sensitive configuration and management features. After successful authentication, the admin can manage and update hospital details, including hospital names, locations, departments, and available facilities. This information helps users easily search and select appropriate hospitals.

In addition, the admin maintains complete records of medical stores, including store names, addresses, available medicines, and contact details. This allows efficient tracking of pharmaceutical resources and improves coordination between hospitals and pharmacies. The admin also manages user details for all system participants, such as patients, doctors, nurses, researchers, and DSP users. By maintaining accurate user records and controlling access privileges, the admin module ensures data integrity, system

security, and smooth operation of the overall healthcare management platform.



5. ID Generation & Data Retrieval Module

Every database uploaded by an operator is assigned a unique blockchain-linked ID for tracking and retrieval. The system generates this ID using SHA-256 hashing of the data and metadata, making it tamper-proof and unique across the blockchain network. Users can later retrieve data by simply entering this ID into the system. The retrieval process verifies the ID against the blockchain ledger to confirm integrity before fetching the corresponding encrypted data blocks. This guarantees that users always access the original and untampered version of the data.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results showed that the system significantly improved the speed and reliability of accessing electronic health records while maintaining strong data privacy and integrity. The optimized database structure enabled faster query processing compared to traditional healthcare data management systems. The analysis confirms that the proposed approach provides a scalable, secure, and efficient solution for medical data sharing across healthcare institutions and supports real-time access to patient information.

Fig. 2: Home Page

Fig. 3: Admin Login

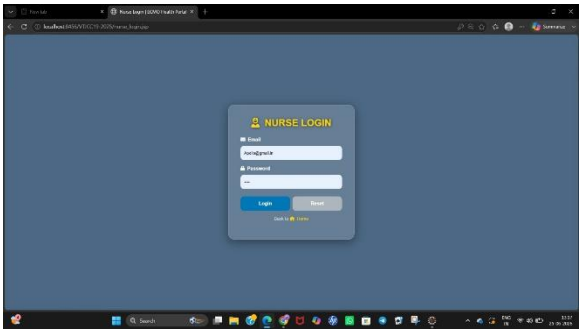


Fig. 4: Nurse Login

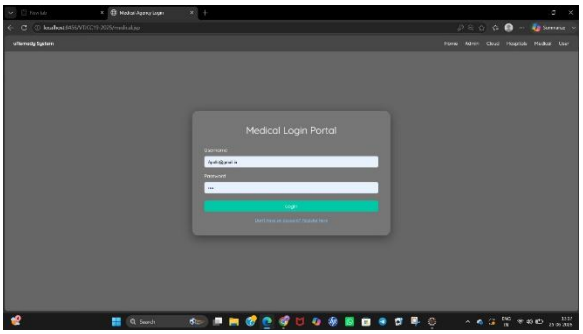


Fig. 5: Medical Login

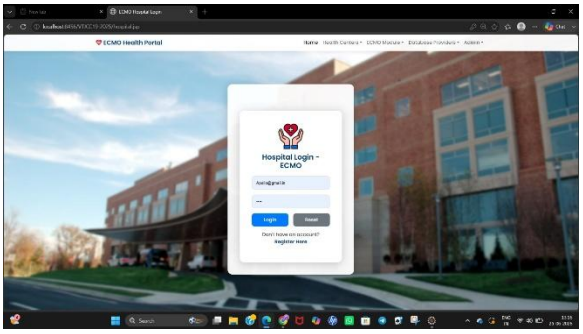


Fig. 6: Hospital Login

V. CONCLUSION

We presented ECMO, a novel protocol for efficient and confidential medical data outsourcing. ECMO combines symmetric encryption, ordered additive secret sharing, and a unique permutation algorithm to address key challenges in medical data security. Our formal security analysis proves that ECMO provides strong guarantees against adversaries controlling up to $n - 1$ database service providers, ensuring both data confidentiality and access pattern privacy. The proposed enhancements, including the proxy-based mechanism, further strengthen ECMO's resilience against potential time-based brute force attacks and other advanced threats. Finally, we conduct extensive experiments, demonstrating ECMO's robustness against strong adversaries, as well as its efficiency and scalability in real-world scenarios.

REFERENCES

[1] A. Hoerbst and E. Ammenwerth, "Electronic health records," Methods Inf. Med., vol. 49, no. 04, pp. 320–336, 2010.

[2] A. K. Jha et al., "Use of electronic health records in us hospitals," New England J. Med., vol. 360, no. 16, pp. 1628–1638, 2009.

[3] R. S. Evans, "Electronic health records: Then, now, and in the future," Yearbook Med. Informat., vol. 25, no. S01, pp. S48–S61, 2016.

[4] B. Brumen et al., "Outsourcing medical data analyses: Can technology overcome legal, privacy, and confidentiality issues," J. Med. Internet Res., vol. 15, no. 12, 2013, Art. no. e2471.

[5] E. Bertino, B. C. Ooi, Y. Yang, and R. H. Deng, "Privacy and ownership preserving of outsourced medical data,"

in Proc. 21st IEEE Int. Conf. Data Eng., 2005, pp. 521–532.

[6] W. Wang, L. Chen, and Q. Zhang, "Outsourcing high-dimensional healthcare data to cloud with personalized privacy preservation," Comput. Netw., vol. 88, pp. 136–148, 2015.

AUTHORS Profile

Mrs. SHANGAM GEETHA has received his B.Tech-Computer Science and Engineering from Nagarjuna institute of technology in 2012, M.Tech degree in Computer Science and Engineering from Vidya Vikas institute of technolog in 2014. She is dedicated to teaching field from the last 9 years. Her research area Quantum Computing and Aptitude Computing . At present she is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus ,Ibrahimpatnam, Telangana, India.

Ms. TUMULURI SAI PRANITHA pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Ms. DUNUKUNALA AKHILA pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Mr. AYIOULU PAVAN pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Mr. AVULA SHIVA KUMAR pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.