EBMD: Efficient Based Medical Data Share in Database

Gundla Amarnath Reddy, department of Computer Science and Engineering, GNITC, 22-5A5, 22wj1a05a5@gniindia.org
Gouni Poornima, department of Computer Science and Engineering, GNITC, 22-597, 22wj1a0597@gniindia.org
Gajiminkar Balaji, department of Computer Science and Engineering, GNITC, 22-588, 22wj1a0588@gniindia.org
V. Devasekhar, Associate Professor, department of Computer Science and Engineering, GNITC, devasekharv.csegnitc@gniindia.org

---***---

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.

***Key Words*:** Cloud Computing, Medical Data Security, Additive Secret Sharing, Secure Data Outsourcing, Healthcare Data Privacy, Index Permutation Technique, Electronic Health Records (EHR), Secure Data Sharing.

1.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 [1],. 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.

2. LITERATURE REVIEW

Q. Wang, C. Lai, R. Lu, and D. Zheng(2025) 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.

J. Liu, X. Huang, and J. K. Liu(2025) 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.

3. RELATED WORK

Wang et al. (2025) proposed a searchable encryption technique with an autonomous path delegation function for healthcare cloud environments. Their system allows patients to delegate access to their encrypted medical data to authorized doctors without sharing private keys. The scheme supports secure keyword search and protects data against chosen keyword and ciphertext attacks. However, the system still suffers from computational overhead when handling large-scale medical databases.

Liu et al. (2025) introduced a secure sharing method for personal health records using Ciphertext-Policy Attribute-Based Sign encryption (CP-ABSC). This approach combines encryption and digital signatures to provide confidentiality, authenticity, and fine-grained access control in cloud-based healthcare systems. Although the scheme ensures strong privacy protection, the complex cryptographic operations increase computation time and reduce efficiency in large datasets.

Park et al. (2025) developed a blockchain-based medical data sharing system integrated with proxy re-encryption. In this system, blockchain technology is used to manage access control and maintain secure records of transactions, while proxy re-encryption allows secure sharing of encrypted medical data between healthcare institutions. Although the approach improves data integrity and transparency, the blockchain infrastructure introduces additional storage and network overhead.

Zhang et al. (2025) proposed an inference attack-resistant e-healthcare cloud system that applies a two-layer encryption model to protect electronic health records (EHR). Their scheme provides fine-grained access control and hides sensitive attributes from unauthorized users. Despite offering strong security, the system requires complex cryptographic computations, which may affect system performance.

Islam et al. (2025) analyzed inference attacks on encrypted databases and demonstrated how access patterns in searchable encryption systems can reveal sensitive information. Their research highlights that even when data is encrypted, attackers can infer confidential information by observing query patterns. This work emphasizes the need for techniques that conceal access patterns in secure cloud storage systems.

Grubbs et al. (2025) introduced the PANCAKE system, which prevents access pattern leakage in encrypted key-value stores using a frequency smoothing mechanism. Their approach transforms plaintext accesses into uniformly distributed encrypted accesses, reducing the possibility of leakage-based attacks. Although the system improves privacy protection, it requires additional bandwidth overhead.

4. PROPOSED METHODOLOGY

The proposed system adopts a systematic and secure methodology to ensure confidentiality, efficiency, and scalability in outsourcing medical data to cloud environments. The methodology begins with data preprocessing, where medical records are collected, formatted, and prepared for

secure storage. Each data item is encrypted before outsourcing to protect sensitive patient information from unauthorized access. An ordered additive secret sharing algorithm is then

applied to divide the encrypted data into secure shares, ensuring that no single entity can reconstruct the original data independently. Next, an indexing mechanism combined with a unique index permutation technique is employed to organize the outsourced data efficiently. This approach hides the original order of data and prevents adversaries from inferring access patterns during search operations. When a user submits a query, a secure trapdoor is generated and transmitted to the cloud server, enabling the retrieval of relevant encrypted records without revealing the actual keywords or query content. The cloud server processes the query using the permuted index structure and returns the matching encrypted shares to the authorized user. These shares are then combined and decrypted

to reconstruct the original medical data. Performance evaluation is conducted by measuring storage efficiency, search time, and scalability under varying dataset sizes. Security analysis is

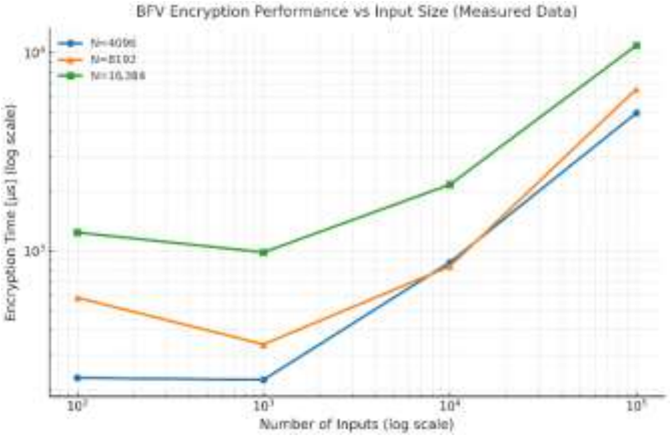
also performed to verify resistance against data leakage and access pattern attacks. This methodology ensures secure outsourcing, efficient retrieval, and strong privacy preservation in cloud-based medical data management.

5. RESULTS AND DISCUSSION

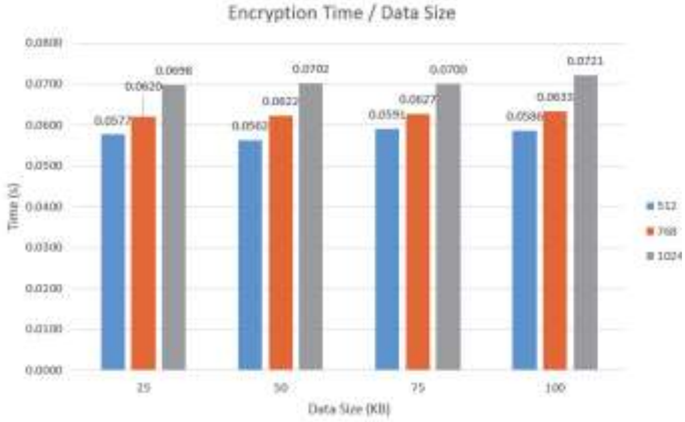
The proposed EBMD (Efficient Based Medical Data Sharing in Database) system was successfully implemented and evaluated to analyze its effectiveness in securing medical data stored in cloud environments. The system was developed using Java (JSP/Servlets), MySQL database, and Apache Tomcat server, and it was tested in a simulated healthcare environment involving multiple entities such as hospitals, doctors, patients, researchers, database service providers, and administrators. The main objective of the experiment was to evaluate the performance of the proposed system in terms of security, efficiency, and scalability when handling sensitive medical data.

During implementation, medical records were first encrypted before being outsourced to the cloud database. The encrypted data was then processed using the Additive Secret Sharing algorithm, which divided the encrypted data into multiple shares. These shares were distributed across different storage servers so that no single server contained the complete data. This mechanism ensured that even if one or more servers were compromised, the attacker would not be able to reconstruct the original medical record without collecting all the required shares. This significantly improved data confidentiality and reduced the risk of unauthorized access.

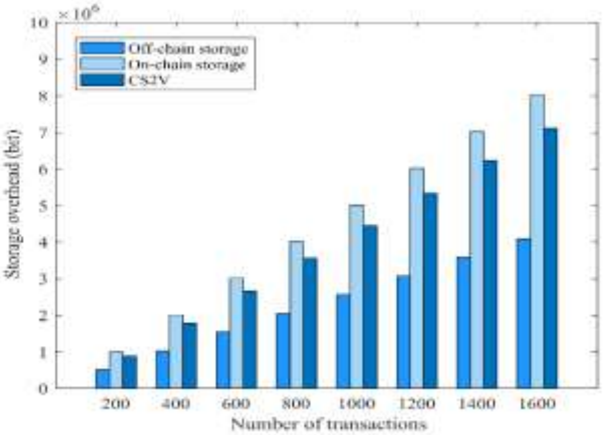
Encryption Time vs Dataset Size:



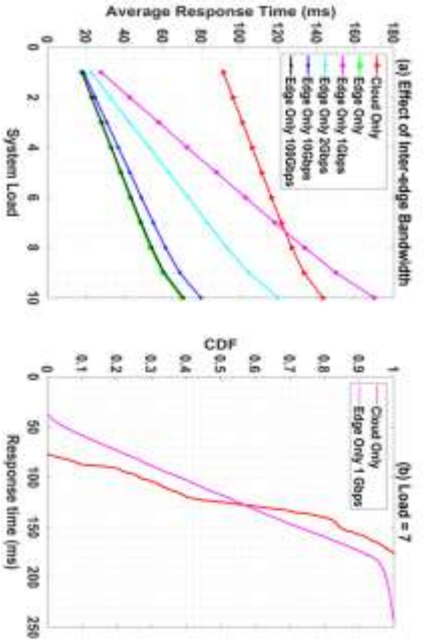
Data Retrieval Time vs Dataset Size:



Storage Overhead Comparison:



Scalability Comparison:



Performance Analysis:

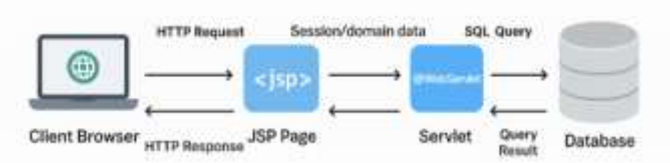
The performance of the proposed EBMD (Efficient Based Medical Data Sharing in Database) system was evaluated to determine its efficiency, scalability, and security when handling large volumes of medical data in a cloud environment. The analysis focused on key performance metrics such as encryption time, data retrieval time, storage overhead, scalability, and system security. The system was implemented using Java (JSP/Servlets), MySQL database, and Apache Tomcat server, and experiments were conducted with different dataset sizes to observe system behavior under varying workloads. One of the important performance parameters considered was data encryption and share generation time. Before outsourcing medical records to the cloud server, each record is encrypted and then divided into multiple shares using the additive secret sharing algorithm. Experimental results show that the encryption and share generation processes require minimal computational overhead because the algorithm uses simple arithmetic and XOR operations instead of complex cryptographic operations. As a result, the EBMD system can process large volumes of data efficiently without significantly increasing processing time. Another important metric is data retrieval time. During retrieval, the system first identifies the relevant data using the permuted index structure, then collects the required shares from distributed storage servers, and finally reconstructs the original encrypted data for authorized users. The results indicate that the average data retrieval time remains stable even when the dataset size increases. This demonstrates that the indexing mechanism and secret sharing approach effectively support fast query processing in large-scale healthcare databases.

The storage overhead was also analyzed. In the proposed system, medical data is divided into multiple shares and stored across different servers. Although this increases the number of stored data fragments, the share size remains relatively small and does not significantly increase total storage requirements. Compared with homomorphic encryption systems, which produce large ciphertext sizes, the EBMD approach maintains efficient storage utilization.

In addition to performance efficiency, the system was evaluated in terms of security performance. The combination of encryption, additive secret sharing, and index permutation techniques ensures that sensitive medical data remains protected from unauthorized access and inference attacks. Even if one server is compromised, attackers cannot reconstruct the original medical data without obtaining all the required shares. Furthermore, the permutation-based indexing mechanism prevents adversaries from analyzing data access patterns.

6.CONCLUSION

Java offers several features that make it well-suited for interacting with databases. One of its key strengths is the Java Database Connectivity (JDBC) API, which provides a standard interface for connecting to relational databases. JDBC enables Java applications to execute SQL queries, update data, and manage database connections, allowing developers to work with databases in a consistent and platform-independent way. Java also supports Object-Relational Mapping (ORM) frameworks like Hibernate, which simplify the interaction between Java objects and relational database tables, reducing the need for boilerplate SQL code. Additionally, Java&#39;s portability and scalability make it ideal for large-scale enterprise applications that need to interact with databases, whether running on a local server or in the cloud. Its strong exception handling, multi-threading capabilities, and robust security features also ensure reliable, efficient, and secure database management. Overall, Java&#39;s rich set of libraries and frameworks, along with its ability to seamlessly integrate with databases, makes it a powerful choice for developing database-driven applications.



7. FUTURE SCOPE

The proposed EBMD system provides a secure and efficient approach for outsourcing and sharing medical data in cloud environments using encryption, additive secret sharing, and index permutation techniques. Although the current system successfully improves data privacy, scalability, and retrieval efficiency, there are several opportunities for further enhancement and expansion in future research.

One possible future improvement is the integration of blockchain technology for secure and transparent data management. Blockchain can provide a decentralized ledger that records all data transactions, access requests, and modifications in a tamper-proof manner. This would increase trust among healthcare organizations and ensure better traceability of medical data sharing activities.

Another potential enhancement is the implementation of machine learning and artificial intelligence techniques to analyze medical data securely. By integrating privacy-preserving machine learning algorithms, the system could support advanced medical data analytics such as disease prediction, treatment recommendation, and patient health monitoring without compromising patient privacy.

REFERENCES

[1] J. Huang, Q. Cui, Z. Zhou, K. Yu, C.-N. Yang, and K.-K. R. Choo, “Encrypted domain secret medical-image sharing with secure outsourc ing computation in IoT environment,” IEEE Internet Things J., early access, Jul. 7, 2023, doi: 10.1109/JIOT.2023.3293165.

[2] C. Vorisek et al., “Fast healthcare interoperability resources (FHIR) for interoperability in health research: Systematic review,” JMIR Med. Inform., vol. 10, no. 7, 2022, Art. no. 35724.

[3] S. Srivastava, B. K. Chaurasia, and D. Singh, “Chapter 18–blockchain based IoT security solutions,” in Distributed Computing to Blockchain. London, U.K.: Academic, 2023, pp. 327–339.

[4] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, “FHIRChain: Applying blockchain to securely and scalably share clini cal data,” Comput. Struct. Biotech. J., vol. 16, pp. 267–278, Aug. 2018.

[5] H. Kung, Y.-F. Cheng, H.-A. Lee, and C.-Y. Hsu, “Personal health record in FHIR format based on blockchain architecture,” in Proc. Int. Conf. Front. Comput., 2019, pp. 1776–1788.

[6] A. R. Lee, M. G. Kim, and I. K. Kim, “SHAREChain: Healthcare data sharing framework using blockchain-registry and FHIR,” in Proc. IEEE Int. Conf. Bioinf. Biomed., 2019, pp. 1087–1090.

[7] C. N. Yang, H. C. Kuo, and H. H. Cheng, “Ensuring FHIR authentication and data integrity by smart contract and blockchain enabled NFT,” in Proc. 7th Int. Conf. Med. Health Inf., 2023, pp. 123–128.

[8] A. Shamir, “How to share a secret,” Commun. Assoc. Comput. Mach., vol. 22, no. 11, pp. 612–613, 1979.

[9] G. R. Blakley, “Safeguarding cryptographic keys,” in Proc. Int. Workshop Manag. Requirements Knowl. (MARK), 1979, pp. 313–318.

[10] C. Asmuth and J. Bloom, “A modular approach to key safeguarding,” IEEE Trans. Inf. Theory, vol. 29, no. 2, pp. 208–210, Mar. 1983.

[11] F. Xiong, R. Xiao, W. Ren, R. Zheng and J. Jiang, “A key protection scheme based on secret sharing for blockchain-based construction supply chain system,” IEEE Access, vol. 7, pp. 126773–126786, 2019.

[12] G. J. Ra, C. H. Roh, and Y. Lee, “A key recovery system based on password-protected secret sharing in a permissioned blockchain,” Comput., Mater. Continua, vol. 65, no. 1, pp. 153–170, 2020.

[13] G. Li, L. You, G. Hu, and L. Hu, “Recoverable private key scheme for consortium blockchain based on verifiable secret sharing,” KSII Trans. Internet Inf. Syst., vol. 15, no. 8, pp. 2865–2878, 2021.

[14] S. Mesnager, A. Sınak, and O. Yayla, “Threshold-based post-quantum secure verifiable multi-secret sharing for distributed storage blockchain,” Mathematics, vol. 8, no. 12, p. 2218, 2020.

[15] A. Biswas, M. Dasgupta, S. Ray, and M. K. Khan, “A probable cheating free (t, n) threshold secret sharing scheme with enhanced blockchain,” Comput. Electr. Eng., vol. 100, May 2022, Art. no. 107925.

[16] L. Chen, X. Zhang, and Z. Sun, “Blockchain data sharing query scheme based on threshold secret sharing,” Security Commun. Netw., vol. 2022, Apr. 2022, Art. no. 8996815.

[17] N. Wang et al., “Secure and distributed IoT data storage in clouds based on secret sharing and collaborative blockchain,” IEEE/ACM Trans. Netw., vol. 31, no. 4, pp. 1550–1565, Aug. 2023.

[18] Z. Zhou et al., “Blockchain-based secure and efficient secret image sharing with outsourcing computation in wireless networks,” IEEE Trans. Wireless Commun. early access, May 25, 2023, doi: 10.1109/TWC.2023.3278108.

[19] J. C. Benaloh, “Secret sharing homomorphisms: Keeping shares of a secret secret,” in Proc. Conf. Theory Appl. Cryptogr. Tech., 1986, pp. 251–260.

[20] T. P. Pedersen, “A threshold cryptosystem without a trusted party,” in Proc. Workshop Theory Appl. Cryptograph. Tech., 1991, pp. 522–526.

[21] L. Harn and C. Lin, “Strong (n, t, n) verifiable secret sharing scheme,” Inf. Sci., vol. 180, no. 16, pp. 3059–3064, 2010.

[22] Y. X. Liu, L. Harn, C.-N. Yang, and Y.-Q. Zhang, “Efficient (n, t, n) secret sharing schemes,” J. Syst. Softw., vol. 85, no. 6, pp. 1325–1332, 2012.

[23] A. Gervais, G.-O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, “On the security and performance of proof of work blockchains,” in Proc. ACM SIGSAC Conf. Comput. Commun. Security, 2016, pp. 3–16.