Review Paper of A Secure Data Sharing And Authorized Searchable Framework For E- Healthcare System

Prof. Ashwini Bhople[1], Ganesh Gajanan Gatmane[2], Pravin Kailas Damdhar[3]
Tejas Anil Hinge[4], Yash Sunil Hinge[5]
[1, 2, 3, 4, 5] Dept of Computer Science Engineering
[1, 2, 3, 4, 5] Padm. Dr. VBKCOE, Malkapur, Maharashtra, India.

Abstract- *Healthcare systems increasingly rely on electronic data for patient records and medical information. Ensuring the security and privacy of this sensitive data is paramount to maintaining trust and confidentiality. This review paper introduces a secure data sharing and authorized searchable framework designed specifically for the E-Healthcare system. The framework addresses the challenges of data sharing and retrieval while prioritizing the protection of patients' sensitive health information. By implementing robust security measures and an authorized searchable mechanism, the proposed framework aims to strike a balance between accessibility and privacy in electronic healthcare environments.*

The first aspect of the framework involves secure data sharing, emphasizing the need for encryption, access controls, and secure communication channels. Protecting health records from unauthorized access is crucial, and the framework explores encryption techniques and access management strategies to mitigate potential breaches. The second aspect focuses on an authorized searchable framework, allowing healthcare professionals to efficiently retrieve relevant information without compromising patient privacy. Through proper authorization mechanisms, the framework ensures that only authorized personnel can access and search for specific health records, maintaining confidentiality while facilitating data retrieval.

In conclusion, this review paper introduces a comprehensive frame work that addresses the dual challenges of secure data sharing and authorized searchable functionalities within the context of E- Healthcare. By incorporating advanced encryption, access controls, and an efficient search mechanism, the proposed framework aims to enhance the overall security and privacy of electronic healthcare data, contributing to the ongoing evolution of secure healthcare information systems.

Keywords- Secure Data Sharing, Authorized Searchable Framework, E-Healthcare System, Privacy, Encryption, Access Controls, Health Information, Electronic Health Records, Data Security, Medical Information.

I. INTRODUCTION

In contemporary healthcare systems, the integration of electronic technologies has revolutionized the storage, management, and accessibility of patient information, giving rise to what is commonly known as E-Healthcare. This paradigm shift offers numerous benefits, including improved efficiency, enhanced communication among healthcare providers, and better patient care coordination. However, along with these advantages come significant challenges, particularly in ensuring the security and privacy of sensitive medical data. As such, there is a growing need for robust frameworks that can safeguard electronic health records (EHRs) while enabling authorized access and efficient information retrieval.

The introduction of electronic health records has ushered in an era of unprecedented convenience and accessibility in healthcare delivery. By digitizing patient information, healthcare providers can access crucial medical data instantaneously, leading to more informed decision-making and streamlined treatment processes. Moreover, E-Healthcare facilitates seamless communication between different healthcare entities, allowing for coordinated care across various medical specialties and geographical locations. However, the widespread adoption of electronic systems also exposes healthcare data to potential security threats and privacy breaches, underscoring the importance of implementing robust security measures.

Despite the benefits of E-Healthcare, concerns regarding data security and patient privacy persist, necessitating the development of innovative solutions to address these challenges. This paper aims to introduce a secure data sharing and authorized searchable framework tailored specifically for the E-Healthcare environment.

By combining advanced encryption techniques, access controls, and efficient search algorithms, the proposed framework seeks to strike a balance between accessibility and confidentiality, ensuring that sensitive medical information remains protected while enabling authorized users to retrieve pertinent data when needed. Through a comprehensive examination of the framework's components and functionalities, this paper aims to provide insights into how modern healthcare systems can leverage technology to enhance security and privacy in electronic data sharing and retrieval processes.

II. PROBLEM FORMULATION

The E-Healthcare landscape faces several critical challenges, particularly in the realms of data security, privacy, and efficient information retrieval. One of the primary issues is the vulnerability of electronic health records (EHRs) to unauthorized access, posing a significant threat to patient confidentiality. As the volume of sensitive medical data stored electronically continues to grow, the risk of security breaches and unauthorized disclosures increases proportionally. The need to strike a delicate balance between providing healthcare professionals with access to relevant patient information and safeguarding the privacy of individuals remains a central problem.

Another aspect of the problem formulation revolves around the complexity of implementing efficient and secure search functionalities within E-Healthcare systems. Traditional search mechanisms often fall short in meeting the specific requirements of healthcare information retrieval, leading to potential delays in accessing critical data. Balancing the need for rapid and accurate searches with the imperative of maintaining stringent access controls is a challenge that demands innovative solutions. The design of a system that allows authorized users to search for and retrieve patient information while upholding the confidentiality and integrity of the data represents a multifaceted problem within the E-Healthcare domain.

Moreover, compliance with regulatory frameworks, such as the Health Insurance Portability and Accountability Act (HIPAA), adds an additional layer of complexity to the problem formulation. Ensuring that the proposed framework aligns with legal and ethical standards, while also addressing the unique challenges posed by the evolving landscape of healthcare technology, is an integral part of problem-solving in this domain. Therefore, the problem formulation encompasses the intricate interplay between security, privacy, and information retrieval efficiency in the context of electronic healthcare systems.

III. PROPOSE SYSTEM METHODOLOGY

The proposed system methodology focuses on addressing the identified challenges in E-Healthcare by introducing a Secure Data Sharing and Authorized Searchable Framework. The system employs a multifaceted approach that integrates robust security measures, efficient data sharing protocols, and an advanced searchable framework to ensure the confidentiality and integrity of patient information.

To initiate this methodology, a comprehensive user authentication and authorization mechanism will be implemented. This involves employing state-of-the-art encryption algorithms to secure user credentials and ensuring that only authorized personnel with the appropriate clearance levels can access the E- Healthcare system. By establishing a stringent access control framework, the system mitigates the risk of unauthorized data access and maintains compliance with regulatory standards such as HIPAA.

Data sharing is a critical component of E-Healthcare, and the proposed methodology incorporates secure sharing protocols. Utilizing encryption techniques, the systemensures end-to-end security during data transmission. Access permissions are dynamically managed to allow healthcare professionals to share specific information based on the patient's consent and the necessity of the situation. This enhances collaboration among healthcare providers while safeguarding patient privacy.

The framework introduces a searchable mechanism that combines efficiency with privacy. Leveraging advanced indexing and search algorithms, the system enables authorized users to perform rapid and accurate searches within the vast repository of electronic health records. The design prioritizes the user experience, ensuring that healthcare professionals can swiftly access pertinent information without compromising the security and privacy of the data.

Furthermore, the system methodology integrates audit trails and monitoring mechanisms. These features allow administrators to track and review user activities within the system, enhancing accountability and transparency. In the event of a security incident or privacy breach, the audit trail facilitates forensic analysis, aiding in the identification of the root cause and implementation of corrective measures.

The proposed system methodology is designed to be scalable and adaptable, accommodating the evolving landscape of E-Healthcare technologies. Regular updates and security patches will be implemented to stay ahead of

emerging threats and ensure the long- term viability and effectiveness of the Secure Data Sharing and Authorized Searchable Framework in the dynamic E-Healthcare environment.

IV. WORKING ON LANGUAGES

The working language for the proposed E-Healthcare system is JAVA, a versatileNand widely-used programming language known for its platform independence and robust features. JAVA provides the necessary flexibility and scalability required for developing complex healthcare systems. Its object-oriented nature facilitates modular design, making it easier to manage and maintain the codebase. The use of JAVA ensures compatibility across different platforms, allowing seamless integration with various healthcare IT environments.

For the development environment, the system leverages Apache IDE and NetBeans 16. Apache IDE, with its integrated development tools, provides a comprehensive and efficient platform for coding, debugging, and testing JAVA applications. NetBeans 16, a well-established integrated development environment, complements Apache IDE by offering a user-friendly interface and additional tools for JAVA development. These integrated development environments streamline the coding process, enhance collaboration among developers, and contribute to the overall efficiency of the system development life cycle.

In terms of data management, the system relies on MYSQL as the backend database. MYSQL is a reliable and widely-used relational database management system that offers excellent performance, data integrity, and scalability. It provides a robust foundation for storing and retrieving patient information securely. The use of MYSQL ensures that the E-Healthcare system can handle the expected volume of data while maintaining the required level of data consistency and security. Overall, the combination of JAVA, Apache IDE, NetBeans 16, and MYSQL establishes a powerful and cohesive development stack for building a secure and efficient E-Healthcare system.

V. RELATED WORKING

The proposed E-Healthcare system builds upon existing research and technologies in the field, taking inspiration and insights from related studies. While specific details about related working are not provided, it's common in academic or research projects to review existing literature and technologies to identify gaps and opportunities for improvement.

In E-Healthcare systems, related work often includes studies on electronic healthrecords(EHRs),telemedicine, health information systems, and data security in healthcare. Researchers may explore how existing systems handle patient data, ensure privacy, and facilitate efficient healthcare delivery.

Additionally, related working might involvb the examination of frameworks or methodologies employed in similar projects. This could include a review of how other healthcare systems have implemented features such as data sharing, authorization mechanisms, and searchable functionalities. Learning from the successes and challenges of similar systems is crucial for refining the proposed methodology and ensuring that the E- Healthcare system aligns with best practices in the field.

Furthermore, related working may encompass advancements in JAVA programming, Apache IDE, NetBeans, and MYSQL databases within the healthcare domain. Staying abreast of the latest technologies and development practices helps in incorporating innovative solutions and ensuring that the proposed E-Healthcare system remains current and effective.

REFERENCES

[1] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, ‘‘Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and exten sions,’’ in Proc. Annu. Int. Cryptol. Conf. Berlin, Germany: Springer, 2005, pp. 205–222.

[2] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, ‘‘Improved proxy re encryption schemes with applications to secure distributed storage,’’ ACM Trans. Inf. Syst. Secur., vol. 9, no. 1, pp. 1–30, 2006.

[3] J. Baek, R. Safavi-Naini, and W. Susilo, ‘‘Public key encryption with keyword search revisited,’’ in Proc. Int. Conf. Comput. Sci. Appl. (ICCSA), 2008, pp. 1249–1259.

[4] T. Bhatia, A. K. Verma, and G. Sharma, ‘‘Towards a secure incremental proxy re-encryption for e- healthcare data sharing in mobile cloud com puting,’’ Concurrency Comput., Pract. Exper., vol. 32, no. 5, p. e5520, Mar. 2020.

[5] T. Bhatia, A. K. Verma, and G. Sharma, ‘‘Secure sharing of mobile personal healthcare records using certificateless proxy re-encryption in cloud,’’ Trans. Emerg.

Telecommun. Technol., vol. 29, no. 6, p. e3309, Jun. 2018.

[6] I. F. Blake, G. Seroussi, and N. Smart, ‘‘Advances in Elliptic Curve Cryptography (London Mathematical Society Lecture Note Series (317)), vol. 19. Cambridge, U.K.: Cambridge Univ. Press, no. 20, 2005, p. 666.

[7] M. Blaze, G. Bleumer, and M. Strauss, ‘‘Divertible protocols and atomic proxy cryptography,’’ in Advances in Cryptology-EUROCRYPT. Berlin, Germany: Springer, 1998, pp. 127–144.

[8] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, ‘‘Public key encryption with keyword search,’’ in Proc. Int. Conf. Theory Appl. Cryptograph. Techn. Berlin, Germany: Springer, 2004, pp. 506–522.

[9] D. Boneh and B. Waters, ‘‘Conjunctive, subset, and range queries on encrypted data,’’ in Proc. Theory Cryptogr. Conf. Berlin, Germany: Springer, 2007, pp. 535–554.

[10] H. Fang, X. Wang, and L. Hanzo, ‘‘Learning-aided physical layer authen tication as an intelligent process,’’ IEEE Trans. Commun., vol. 67, no. 3, pp. 2260–2273, Mar. 2019.

[11] H. Fang, L. Xu, and X. Wang, ‘‘Coordinated multiple-relays based physical-layer security improvement: A single-leader multiple-followers Stackelberg game scheme,’’ IEEE Trans. Inf. Forensics Security, vol. 13, no. 1, pp. 197–209, Jan. 2018.

[12] L. Fang, W. Susilo, C. Ge, and J. Wang, ‘‘Chosen-ciphertext secure anonymous conditional proxy re-encryption with keyword search,’’ Theor. Comput. Sci., vol. 462, pp. 39–58, Nov. 2012.

[13] L. Fang, J. Wang, C. Ge, and Y. Ren, ‘‘Fuzzy conditional proxy re encryption,’’ Sci. China Inf. Sci., vol. 56, no. 5, pp. 1–13, May 2013.

[14] J. Feng, L. T. Yang, R. Zhang, W. Qiang, and J. Chen, ‘‘Privacy preserv ing high-order bi-Lanczos in cloud-fog computing for industrial appli cations,’’ IEEE Trans. Ind. Informat., early access, May 28, 2020, doi: 10.1109/TII.2020.2998086.

[15] J. Feng, L. T. Yang, Q. Zhu, and K.-K.-R. Choo, ‘‘Privacy-preserving tensor decomposition over encrypted data in a federated cloud environment,’’ IEEE Trans. Dependable Secure Comput., vol. 17, no. 4, pp.b 857–868, Jul. 2020.

[16] [16] J.-S. Fu, Y. Liu, H.-C. Chao, B. K. Bhargava, and Z.-J. Zhang, ‘‘Secure data storage and searching for industrial IoT by integrating fog comput ing and cloud computing,’’ IEEE Trans. Ind. Informat., vol. 14, no. 10, pp. 4519–4528, Oct. 2018.

[17] M. Green and G. Ateniese, ‘‘Identity-based proxy re-encryption,’’ in Applied Cryptography and Network Security. Berlin, Germany: Springer, 2007, pp. 288–306.

[18] D. He, M. Ma, S. Zeadally, N. Kumar, and K. Liang, ‘‘Certificateless public key authenticated encryption with keyword search for industrial Internet of Things,’’ IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3618–3627, Aug. 2018.

[19] Y. J. He, T. W. Chim, L. C. K. Hui, and S.-M. Yiu, ‘‘Non-transferable proxy re-encryption scheme for data dissemination control,’’ IACR Cryp tol. ePrint Arch., vol. 2010, p. 192, Jan. 2010.

[20] Q. Huang, L. Wang, and Y. Yang, ‘‘Secure and privacy-preserving data sharing and collaboration in mobile healthcare social networks of smart cities,’’ Secur. Commun. Netw., vol. 2017, pp. 1–12, Aug. 2017.

[21] Q. Huang, Y. Yang, and J. Fu, ‘‘PRECISE: Identity-based private data sharing with conditional proxy re-encryption in online social networks,’’ Future Gener. Comput. Syst., vol. 86, pp. 1523–1533, Sep. 2018.

[22] B. Lynn. (2006). PBC Library. [Online]. Available: http://crypto. stanford.edu/pbc

[23] M. Ma, D. He, D. Kumar, K.-K. R. Choo, and J. Chen, ‘‘Certificateless searchable public key encryption scheme for industrial Internet of Things,’’ IEEE Trans. Ind. Informat., vol. 14, no. 2, pp. 759–767, May 2017.

[24] Y. Miao, J. Ma, X. Liu, F. Wei, Z. Liu, and X. A. Wang, ‘‘m2-ABKS: Attribute-based multi-keyword search over encrypted personal health records in multi- owner setting,’’ J. Med. Syst., vol. 40, no. 11, p. 246, Nov. 2016.

[25] M. Naz, F. A. Al-zahrani, R. Khalid, N. Javaid, A. M. Qamar, M. K. Afzal, and M. Shafiq, ‘‘A secure data sharing platform using blockchain and interplanetary file system,’’ Sustainability, vol. 11, no. 24, p. 7054,2019.