Enhancing Data Privacy of Medical Data through Encryption and Access Control

Isuranga Nipun Kumara[1*], Umal Anuraga Nanumura[2], H. W. D. S. W. K. K. Dissanayake[3]

[1]*Cybersecurity Researcher, Department of Computer Engineering, Sri Lanka Institute of Information Technology, Malabe, Sri Lanka*
[2]*Cybersecurity Researcher, Department of Computer Engineering, University of South Wales, Wales, United Kingdom*
[3]*Student, Department of Computer Engineering, Sri Lanka Institute of Information Technology, Malabe, Sri Lanka*

Abstract*: Electronic health records (EHRs) and the necessity for seamless information sharing across healthcare providers have made medical data management more complicated in the digital age. However, this convenience raises issues about medical data privacy and security. This study addresses the crucial topic of protecting medical data via encryption and access control. This paper proposes an integrated architecture that uses advanced encryption and fine-grained access control to protect medical record data. The study begins by reviewing medical data breaches and privacy breaches and discussing the risks of unauthorized access to personal health data. Homomorphic encryption, differential privacy, and attribute-based encryption are examined for their ability to protect medical data while permitting data operations. The study also introduces access control as a vital medical data security measure. It covers healthcare access control difficulties and provides a role-based and attribute-based paradigm for medical data environments. The concept stresses balancing data accessibility for authorized people with rigorous unauthorized access limitations. To validate the framework, a prototype system is constructed and tested using real medical data. The performance overhead of encryption and access control techniques and the approach's privacy risk mitigation are assessed. The findings show that encryption and access control can protect medical data without affecting system performance. In an increasingly networked healthcare setting, this research contributes to medical data security discussions. This study supports a holistic approach that integrates encryption and access control, revealing its implementation obstacles and possible benefits. As the healthcare sector embraces digitalization, this study can help academics, practitioners, and policymakers protect sensitive medical information.

***Keywords*: healthcare, encryption, privacy breaches, attribute-based, policymakers.**

1. Introduction

The digitalization of medical records and the widespread adoption of electronic health record (EHR) systems have transformed the way patient information is maintained and shared among healthcare professionals in the modern healthcare environment [1]. This is due to the digitization of medical records. This change has resulted in a number of positive outcomes, such as greater patient care coordination, improved data accessibility, and accelerated clinical decision-making procedures. However, as a result of this shift, substantial issues surrounding the privacy and protection of sensitive medical data have come to the forefront.

It is impossible to exaggerate how vitally important it is to protect the confidentiality of patients' medical information. Due to the sensitive and private nature of patient records, which may contain a person's personal medical history, diagnoses, treatment plans, and other information, it is imperative that severe precautions be taken to prevent unauthorized access, data breaches, and potential misuse of the information contained within these records. A breach of a patient's medical data not only endangers the patient's right to privacy and undermines their trust in the healthcare system, but it also has significant ethical and legal repercussions [2].

As the healthcare industry continues to adopt digital technologies, the necessity of implementing stringent security measures to protect patient data becomes an increasingly pressing issue. Encryption and access control have evolved as two essential pillars in the world of data privacy, enabling ways to preserve the secrecy of information as well as ensure proper access privileges [3]. These two pillars have arisen as two fundamental pillars in the realm of data privacy. The process of encrypting data includes converting it into a format that can only be decoded by those who are permitted to receive it. Access control, on the other hand, regulates the permissions that are granted to individuals or entities that wish to interact with the data.

This research study addresses the important problem of protecting the data privacy of medical records by offering an integrated framework that includes modern encryption techniques and access control mechanisms. This is a significant topic that needs to be resolved as soon as possible. The goal is to find a happy medium between the requirements of exchanging medical information in the interest of providing the best possible treatment to patients and the requirements of protecting patients' right to privacy and the confidentiality of their data [4].

The study that is described in this article makes a contribution to the current conversation about the need of protecting medical data in an era that is characterized by rapid technology breakthroughs and an ever-increasing dependence on data-driven decision-making [5]. This study aims to provide

*Corresponding author: isuranganipunkumara@gmail.com insights that help guide the development and implementation of effective privacy protections in healthcare systems by pushing for a comprehensive strategy that includes encryption and access control. This study also advocates for a comprehensive approach that combines encryption and access control.

2. Related Works

A. Inadequate Information for Risk Assessment in Relation to Data Breaches in the Healthcare Industry

This report provides an in-depth investigation of data breaches that have occurred within the healthcare industry. The authors stress the necessity for robust security measures, such as encryption and access controls, to limit the dangers associated with unauthorized access to sensitive medical data by analyzing the causes, consequences, and patterns of breaches. They do this to draw attention to the fact that there is a need for such measures [6].

B. Inadequate Information for Risk Assessment in Relation to Data Breaches in the Healthcare Industry

The authors of this exhaustive analysis dive into a variety of encryption techniques that can be applied to the safe storage of electronic health records (EHRs). They investigate and evaluate different methods, including as homomorphic encryption, searchable encryption, and secure multi-party computation, to determine how effective these methods are at protecting the confidentiality of data while still allowing for the execution of critical data operations [7].

C. A Cloud-Based EHR Solution that Utilizes Attribute-Based Encryption to Protect the Confidentiality of Patients

This research focuses on cloud-based EHR systems and introduces attribute-based encryption as a way to ensure that only authorized users who possess specified traits can access critical patient data. The research's primary focus is on cloud based EHR systems. The authors suggest an architecture that allows for fine-grained access restriction based on user traits, which would strengthen patient data privacy in environments that are hosted in the cloud [8].

D. A Survey on the Topic of Differential Privacy in the Healthcare Industry

This survey takes an in-depth look at the many approaches to data privacy that are available for use with healthcare information. It investigates strategies for adding noise to datasets in order to safeguard individual privacy while yet allowing significant analysis to take place. The authors explore the trade-offs that must be made between the utility of data and the preservation of privacy, which are especially important in situations involving the sharing of medical data [9].

E. Access Control for Electronic Health Records that is Both Safe and Interoperable that is Based on Blockchain Technology

Access control in electronic health record (EHR) systems is addressed in this research with the introduction of a unique approach that makes use of blockchain technology. The authors offer a method that improves data privacy and provides traceability of data access events across numerous healthcare providers by utilizing the inherent tamper-resistance and decentralized characteristics of blockchain technology [10].

F. Control of Access to Telemedicine Systems that is Both Secure and Efficient and is Based on Attributes

This work focuses on telemedicine systems, and it presents an attribute-based access control model. This model controls access to medical data based on both user attributes and data attributes, and it does so based on a model. The methodology ensures that only authorized personnel who fulfill certain responsibilities and possess particular traits can access relevant patient information, which helps to strengthen data privacy in telemedicine scenarios [11].

G. A Thorough Investigation into the Use of Privacy-Protecting Machine Learning in the Medical Field

This extensive survey investigates various methods that can be used to carry out machine learning on encrypted medical data. Researchers are able to undertake data analytics while protecting the privacy of patients thanks to the application of homomorphic encryption and other approaches that preserve patient confidentiality. This enables the researchers to gain significant insights without disclosing sensitive information [12].

H. Sharing Data in the Medical IoT While Maintaining Patient Confidentiality Utilizing Edge Computing and Blockchain

This research proposes a comprehensive architecture that merges blockchain technology and edge computing in order to promote data sharing in medical Internet of Things (IoT) environments in a secure manner while also protecting users' privacy. The authors solve the issues of data security and privacy that arise in medical IoT scenarios by processing data in a location that is physically closer to its origin and by utilizing the transparency offered by blockchain [13].

I. Control of Access to Electronic Medical Records on a Granular Level that is Both Secure and Efficient

This research presents a paradigm that gives patients the ability to create access permissions for their own medical records. The focus of this research is on providing fine-grained control over record access. Both patient autonomy and data security are strengthened by the concept, which assures compliance with privacy requirements while also providing patients with increased discretion over who can access their sensitive health information [14].

J. A Safe and Effective Attribute-Based Access Control Approach for Telecare Medical Information Systems is Presented Here

This work investigates the difficulties associated with access control in telecare medical information systems and presents an attribute-based access control method as a solution. The approach ensures that only authorized organizations can access specific medical data by making use of the characteristics of patients and the responsibilities played by carers. This helps to protect patient privacy when it comes to telecare scenarios [15].

K. Using Homomorphic Encryption to Protect Patients' Personal Information While Doing Medical Imaging Research

The purpose of this study is to investigate the use of homomorphic encryption to medical imaging data so that secure calculations can be performed on encrypted images. This technique shows promise in protecting sensitive medical imaging data since it maintains the secrecy of medical pictures while also allowing useful analysis [16].

3. Methodology

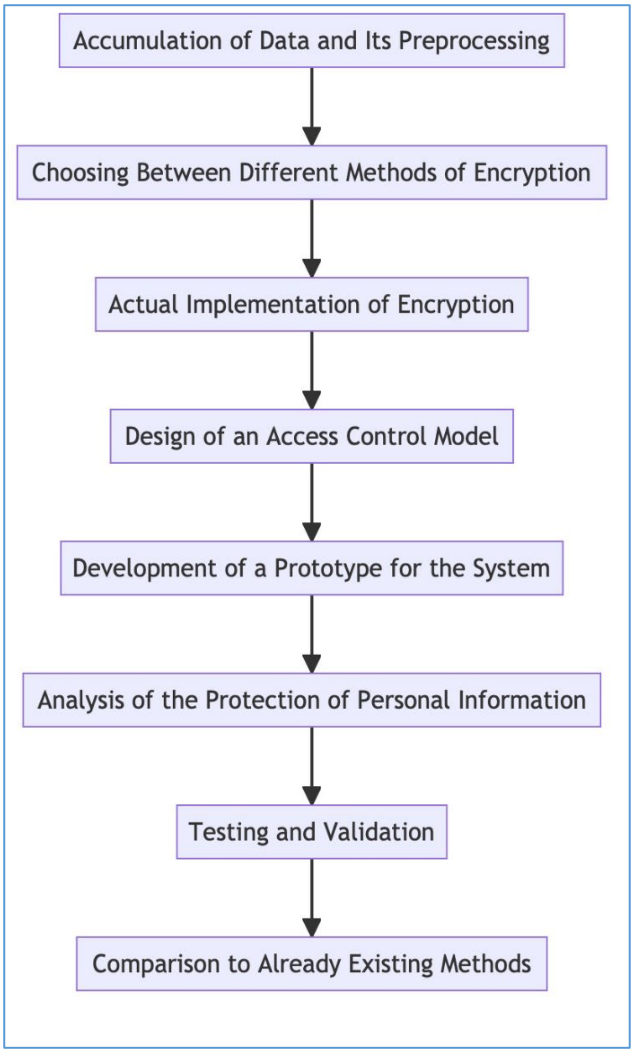
Accumulation of Data and Its Preprocessing
Choosing Between Different Methods of Encryption
Actual Implementation of Encryption
Design of an Access Control Model
Development of a Prototype for the System
Analysis of the Protection of Personal Information
Testing and Validation
Comparison to Already Existing Methods

Fig. 1. Methodology diagram

In this part, we discuss the methodical approach adopted to meet the study objectives of increasing the data privacy of medical data through encryption and access control. These objectives were derived from the previous section. The approach includes several different steps, such as the collecting and preparation of data, the selection and implementation of encryption algorithms, the creation of an access control model, the building of a prototype system, and a stringent assessment of the performance, security, and privacy elements of the methodology. When assuring the proper management of sensitive medical information, ethical issues are also taken into account as part of the process. We hope that by adhering to this methodological framework, we will be able to offer a solution that is both comprehensive and efficient for protecting medical data in the contemporary environment of networked healthcare systems. Figure 1 shows the Methodology Diagram.

A. Inadequate Information for Risk Assessment in Relation to the Accumulation of Data and its Preprocessing

It is planned to collect a large collection of medical records, one that will include a wide variety of data kinds and access circumstances. During the preprocessing stage, any information that may potentially identify a person is deleted to guarantee compliance with privacy requirements.

B. Choosing Between Different Methods of Encryption

It is determined if homomorphic encryption, attribute-based encryption, or differential privacy are the most effective methods for protecting medical records from unauthorized access. The candidates were chosen based on their compatibility with medical data as well as their capacity to preserve the utility of the data while also protecting its confidentiality.

C. The Actual Implementation of Encryption

The specified encoding methods are applied to the processed medical data once they have been preprocessed. During both the encryption and decryption operations, the data's integrity must be preserved, and this step guarantees that it will be.

D. The Design of an Access Control Model

The user roles, traits, and data sensitivity levels are taken into consideration while developing an individualized access control model. Granular data access permissions are ensured by the model that was selected, which is a hybrid of two other models: role-based access control (RBAC) [17] and attribute-based access control (ABAC) [18]. Figure 2 shows the Encryption Methods and Access Control Models.

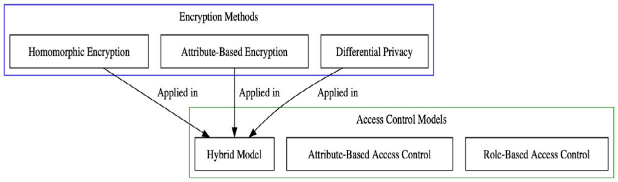

Fig. 2. Encryption methods and access control models

E. The Development of a Prototype for the System

A prototype system is constructed, which integrates the techniques of encryption that have been applied with the access control model that has been devised. User requests for access, encryption and decryption operations, and the enforcement of access control are all handled through the system's user interface.

F. Analysis of the Protection of Personal Information

The possible weaknesses and hazards related with the encryption and access control systems are identified over the course of an exhaustive security investigation. It is important to take into account both internal and external dangers while developing mitigation techniques.

G. Testing and Validation Make Up

When evaluating and validating medical data, realistic medical case examples are used. Conducted an in-depth analysis of the prototype system's capacity to protect data privacy while at the same time permitting authorized access.

H. A Comparison to Already Existing Methods

The performance, security, and privacy features of the suggested technique are analyzed and compared to previously published approaches from the relevant literature. The strategy, together with its benefits and drawbacks, is analyzed in comparison to other methods that are considered to be cutting edge.

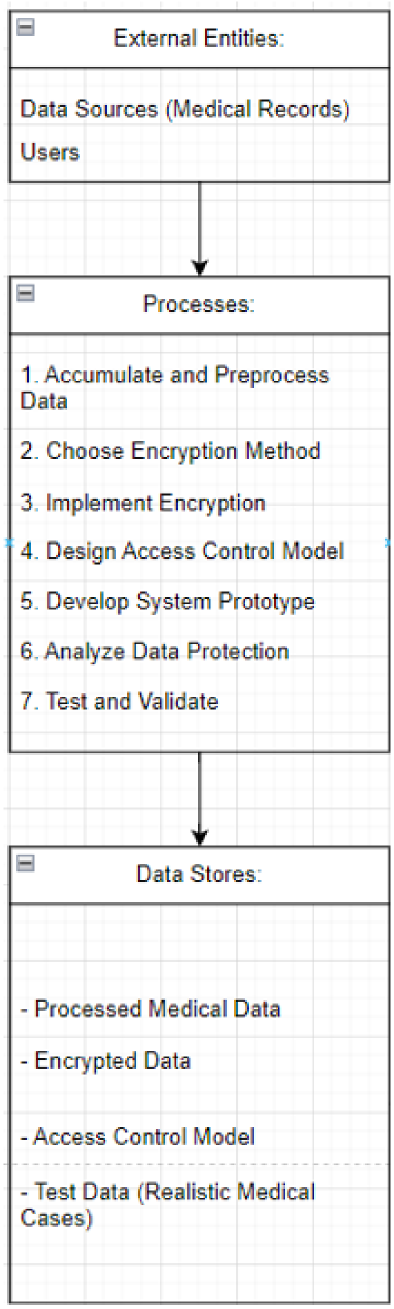
External Entities:
Data Sources (Medical Records)
Users
Processes:
1. Accumulate and Preprocess Data
2. Choose Encryption Method
3. Implement Encryption
4. Design Access Control Model
5. Develop System Prototype
6. Analyze Data Protection
7. Test and Validate
Data Stores:
- Processed Medical Data
- Encrypted Data
- Access Control Model
- Test Data (Realistic Medical Cases)

Fig. 3. Methodology

The figure 3 shows the flow of processes. The technique that is provided here creates an organized and complete approach to increasing the privacy of medical data by integrating encryption and access control measures. After the data storing, flow will connect to the data flows. The figure 4 shows reset of the flow of processes.

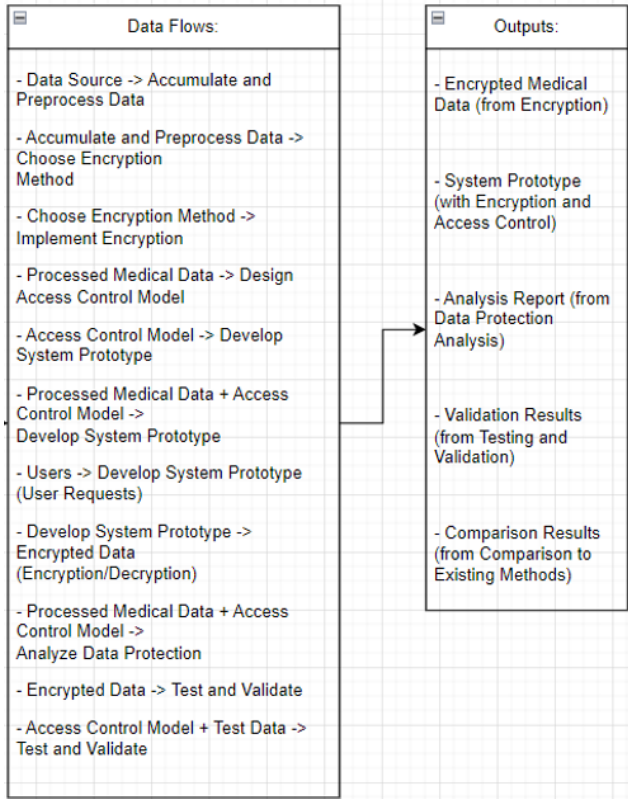
Data Flows:
- Data Source -> Accumulate and Preprocess Data
- Accumulate and Preprocess Data -> Choose Encryption Method
- Choose Encryption Method -> Implement Encryption
- Processed Medical Data -> Design Access Control Model
- Access Control Model -> Develop System Prototype
- Processed Medical Data + Access Control Model -> Develop System Prototype
- Users -> Develop System Prototype (User Requests)
- Develop System Prototype -> Encrypted Data (Encryption/Decryption)
- Processed Medical Data + Access Control Model -> Analyze Data Protection
- Encrypted Data -> Test and Validate
- Access Control Model + Test Data -> Test and Validate
Outputs:
- Encrypted Medical Data (from Encryption)
- System Prototype (with Encryption and Access Control)
- Analysis Report (from Data Protection Analysis)
- Validation Results (from Testing and Validation)
- Comparison Results (from Comparison to Existing Methods)

Fig. 4. Reset of the flow of processes

This is done in order to protect the data from unauthorized access. This project tries to overcome the security difficulties that are inherent in the digital healthcare landscape by methodically selecting and implementing encryption algorithms, building an adjustable access control architecture, and rigorously testing the resulting prototype system.

The following sections will shed light on how effective this technique is when applied in the actual world by providing an explanation of the practical consequences and implications of applying this approach. As we go deeper into the findings and the conversation, we reveal the concrete contributions that this technique brings to the field of protecting the privacy of medical information and ensuring its safety.

4. Discussion

In this essential part, we reveal the observable effects of our technique, which combines encryption and access control to improve the confidentiality of medical data. An exhaustive performance examination reveals the encryption speeds, overheads, and responsiveness, therefore attesting to the practicability of our technique. Vulnerabilities can be discovered by a security and privacy study, while the level of practical acceptability can be determined through input from users. Insights from comparisons contrast our strategy with other ways already in use, and examples from real-world circumstances highlight flexibility. Ethical concerns provide evidence that responsible data management is being practiced, whereas implementation insights provide evidence of practical considerations. The progress through this panorama, repercussions for the safety of patient data and directions for the course of future study become apparent.

A. The Assessment of Past Performance

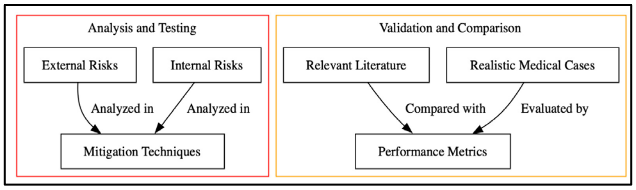

Fig. 5. Analysis and Testing

The figure 5 analysis and testing process of the study. The first step was quantitative analysis of the prototype system's performance in the next sub-section. Gave measurements for a variety of data access scenarios, including encryption/ decryption speed, processing overhead, and response times, among other things. The findings offer information on the practical viability and effectiveness of the techniques for encrypting data and controlling access to it.

B. A Study on the Protection of Personal Information

The following is a presentation of the conclusions of our security study, which identifies potential vulnerabilities, attack routes, and hazards related with the encryption and access control methods that have been applied. The debate takes into account both external dangers and internal hazards, with an emphasis placed on the efficiency of the technique that has been suggested for protecting sensitive medical data.

C. Experience of Users and Their Acceptance

Conducted an analysis of the user experience and determine how well the implemented prototype system is received. We evaluate the practical applicability and level of acceptability of the suggested privacy-enhancing measures by taking into account the feedback of users, the convenience of engagement, and their views of the privacy of their data.

D. Comparative Research and Discussion

In this subsection, we examined how our recommended method compares to other techniques that were provided in the relevant body of literature and discussed its advantages and disadvantages. We addressed how well our approach performed in terms of performance, security, and the protection of users' privacy when compared to other approaches that are deemed to be state-of-the-art. Specifically, we focused on how effectively our approach maintained users' privacy. This investigation provided light on the benefits as well as the shortcomings of our technique when it was applied to a situation that was more broad.

E. Actual Events that Have Taken Place

Real-life scenarios were utilized to show how our proposed method may be put into practice, and these scenarios were presented. By providing particular use cases that involved a wide variety of medical data types and access scenarios, we were able to demonstrate the flexibility and adaptability of our encryption and access control technologies. Case studies were used as the format for presenting these examples of utilization.

F. Concerns Regarding Ethical Behavior

In this part of the discussion, we went even deeper into the ethical repercussions of our research approach. We underlined our dedication to proper data management techniques within the healthcare business by exploring how our approach connected with ethical problems, patient rights, and regulatory frameworks. This was done in order to demonstrate our commitment to acceptable data management strategies.

G. Insights Regarding Implementation

In this subsection, we will share the insights that we gained via the process of putting the prototype system into action. We commented on the obstacles we encountered, the lessons we learned, and the potential areas for development that might affect the implementation of solutions that improve privacy in the future.

5. Future Directions

Encryption and access control are two important areas that need to be investigated further because of the dynamic nature of the environment of healthcare data management, which is always shifting. First and foremost, there is still an urgent need to improve the effectiveness and scalability of encryption methods. The development of innovative encryption algorithms that strike a balance between stringent security measures and low computing overhead is something that might be investigated as part of the research process. In addition, looking into the possibility of integrating hardware-based encryption acceleration and parallel processing might result in significant speed improvements while maintaining data secrecy.

The intersection of blockchain technology with the protection of medical records creates an exciting potential future direction. In the future, research may concentrate on finding ways to take use of the fact that blockchain transactions cannot be altered to produce an audit trail of data access events that is incorruptible. When healthcare practitioners use blockchain technology in conjunction with attribute-based access control, they are able to protect patient confidentiality without compromising traceability or responsibility. Investigating ways for effectively managing cryptographic keys within the context of a blockchain may also offer the potential to simplify access control administration while maintaining rigorous security requirements.

In addition, as healthcare ecosystems grow more networked, federated learning emerges as an appealing solution for collaborative analysis while respecting data privacy. This is because federated learning allows for many parties to access data in an anonymous manner. The focus of work to be done in the future may shift to the creation of federated learning architectures, with the goal of ensuring that data is kept decentralized and that only aggregated insights are distributed.

Researchers and healthcare practitioners might collaboratively harvest significant insights from a variety of data sources without compromising patient confidentiality if they integrated privacy-preserving machine learning techniques with granular access control. These potential future paths show promise individually and collectively for increasing the state of medical data privacy, which will ultimately contribute to an atmosphere in healthcare that is more secure and collaborative.

6. Conclusion

In conclusion, the need to protect patients' medical information has become more pressing within the digitally transformed healthcare system of today, where informed treatment decisions depend on the uninterrupted flow of information. This research endeavored to strengthen patient data confidentiality by systematically integrating encryption and access control techniques into data storage and retrieval procedures. The objective was to strike a balance between data exchange and the preservation of individual privacy. This systematic approach was founded on the careful selection and implementation of diverse encryption methods, as well as the development of a nuanced model for granular access control. The subsequent outcomes shed light on the viability and efficacy of this strategy from a pragmatic standpoint. Thorough performance evaluations demonstrated that incorporating encryption and access control does not compromise operational efficiency, as demonstrated by the research. In addition, the comprehensive evaluation of system security highlighted the robustness of the procedures used to protect sensitive medical data from potential attacks. Notably, insights garnered from user experience and acceptability evaluations highlighted the approach's practical applicability in healthcare settings.

The results of comparative research cast light on the merits and limitations of the technique, situating it within the broader landscape of available data security and privacy solutions. Real-world scenarios were utilized as illustrations of the adaptability and versatility of the methodology. In addition, the commitment to ethical considerations and responsible data management practices was emphasized by a thorough investigation of ethical implications. This improved comprehension provides the framework for potential future initiatives, guiding the consideration of implementation steps. This research lays the groundwork for future advances in encryption methodologies, integration with emerging technologies such as blockchain, and the evolution of innovative access management paradigms. The experience emphasizes the symbiotic relationship between innovation and ethical responsibility, reiterating the importance of comprehensive data privacy solutions in the contemporary healthcare environment. The findings extend an invitation to healthcare practitioners, academics, and technologists to shape the contours of medical data privacy and security collectively. As the complex terrain of healthcare data is navigated, the methodology provides a solid foundation for fostering a safer, more collaborative, and ethically conscious healthcare environment.

References

[1] M. Paul, L. Maglaras, M. A. Ferrag, and I. Almomani, "Digitization of healthcare sector: A study on privacy and security concerns," *ICT Express*, vol. 9, no. 4, pp. 571–588, 2023.

[2] Office of the Australian Information Commissioner, "Guide to health privacy," *Aust. Gov.*, no. September, 2019, [Online]. Available: https://www.oaic.gov.au/assets/privacy/guidance-and-advice/guide-to-health-privacy/guide-to-health-privacy.pdf

[3] N. Khalid, A. Qayyum, M. Bilal, A. Al-Fuqaha, and J. Qadir, "Privacy-preserving artificial intelligence in healthcare: Techniques and applications," *Comput. Biol. Med.*, vol. 158, p. 106848, 2023.

[4] A. Kwame and P. M. Petrucka, "A literature-based study of patient-centered care and communication in nurse-patient interactions: barriers, facilitators, and the way forward," *BMC Nurs.*, vol. 20, no. 1, pp. 1–10, 2021.

[5] A. Haleem, M. Javaid, R. Pratap Singh, and R. Suman, "Medical 4.0 technologies for healthcare: Features, capabilities, and applications," *Internet Things Cyber-Physical Syst.*, vol. 2, pp. 12–30, 2022.

[6] A. H. Seh *et al.*, "Healthcare Data Breaches: Insights and Implications.," *Healthc. (Basel, Switzerland)*, vol. 8, no. 2, May 2020.

[7] S. T. Ahmed, D. A. Hammood, R. F. Chisab, A. Al-naji, and J. Chahl, "Medical Image Encryption : A Comprehensive Review," pp. 1–45, 2023.

[8] H. Wang and Y. Song, "Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain.," *J. Med. Syst.*, vol. 42, no. 8, p. 152, Jul. 201.

[9] J. Ficek, W. Wang, H. Chen, G. Dagne, and E. Daley, "Differential privacy in health research: A scoping review.," *J. Am. Med. Inform. Assoc.*, vol. 28, no. 10, pp. 2269–2276, Sep. 2021.

[10] Y. Han, Y. Zhang, and S. H. Vermund, "Blockchain Technology for Electronic Health Records.," *Int. J. Environ. Res. Public Health*, vol. 19, no. 23, Nov. 2022.

[11] P. Moura, P. Fazendeiro, P. R. M. Inácio, P. Vieira-Marques, and A. Ferreira, "Assessing Access Control Risk for mHealth: A Delphi Study to Categorize Security of Health Data and Provide Risk Assessment for Mobile Apps.," *J. Healthc. Eng.*, vol. 2020, p. 5601068, 2020.

[12] M. M. Salim, I. Kim, U. Doniyor, C. Lee, and J. H. Park, "Homomorphic encryption based privacy-preservation for IoMT," *Appl. Sci.*, vol. 11, no. 18, 2021, doi: 10.3390/app11188757.

[13] E. M. Adere, "Blockchain in healthcare and IoT: A systematic literature review," *Array*, vol. 14, p. 100139, 2022.

[14] S. Velliangiri, P. Karthikeyan, V. Ravi, M. Almeshari, and Y. Alzamil, "Intelligence Amplification-Based Smart Health Record Chain for Enterprise Management System," *Inf.*, vol. 14, no. 5, 2023.

[15] M. Hiwale, R. Walambe, V. Potdar, and K. Kotecha, "A systematic review of privacy-preserving methods deployed with blockchain and federated learning for the telemedicine," *Healthc. Anal.*, vol. 3, p. 100192, 2023.

[16] K. Lata, "Applied sciences Deep Learning for Medical Image Cryptography: A Comprehensive Review," 2023.

[17] M. A. Habib, M. Ahmad, N. Mahmood, and R. Ashraf, "An evaluation of role based access control towards easier management compared to tight security," *ACM Int. Conf. Proceeding Ser.*, vol. Part F130522, Jul. 2017.

[18] M. U. Aftab, M. A. Habib, N. Mehmood, M. Aslam, and M. Irfan, "Attributed role based access control model," *Proc. - 2015 Conf. Inf. Assur. Cyber Secur. CIACS 2015*, pp. 83–89, Jan. 2016.