2025 International Conference on Data Science, Agents, and Artificial Intelligence (ICDSAAI 2025)
28-29 March 2025, Chennai, India

2025 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI) | 979-8-3315-3755-5/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICDSAAI65575.2025.11011747

Enhancing Healthcare Data Security and Privacy through AI-Driven Encryption and Privacy-Preserving Techniques

Dilli Ganesh V*
Department of Mechanical Engineering
Saveetha School of Engineering,
Saveetha Institute of Medical and Technical Sciences(SIMATS)
Chennai, Tamil Nadu, India
dilliganesh001@gmail.com

R M Bommi
Department of Electronics and Communication Engineering
Chennai Institute of Technology
Chennai, India
rmbommi@gmail.com

Nandhini T J
Department of Computer Science and Engineering
Saveetha School of Engineering,
Saveetha Institute of Medical and Technical Sciences(SIMATS)
Chennai, Tamil Nadu, India
nandhinitj67@gmail.com

***Abstract*—The use of digital patient data in health management to meet scientific and analytical requirements is now well established, while ensuring the confidentiality and availability of patient information has emerged as a significant issue. The suggested approach is to integrate AI with the traditional encryption techniques to produce a blend of qualitative and automated encryption methods thus making a dynamic encryption environment that adapts with the level of data sensitivity and the kind of users' access. Furthermore, the approach also incorporate the use of privacy-preserving methodologies including differential privacy, federated learning, and homomorphic encryption, to allow collaboration in the analysis and research of patient data in a more secure manner while preserving the patient's privacy. The methodology also involves the use of artificial intelligence for intrusion detection and also compliance management to guarantee sustained compliance and security, and legal frameworks including HIPAA, GDPR. The findings of the evaluation show that with the help of the proposed AI-based encryption, it is possible to achieve better security outcomes compared with common methods and reduce the probability of both privacy threats and false alarm violations while enhancing the system's performance. Additionally, compliance works well to automate the compliance jobs and relieve the healthcare organizations from the time-consuming duties. Naturally, this work presents a robust, and scalable means of protecting healthcare data while at the same time ensuring that the data can still be processed in a manner that benefits the healthcare system.**

Keywords—AI-driven encryption, healthcare data security, privacy-preserving techniques, differential privacy, federated learning.

I. Introduction

Getting to the modern world advanced in technical in the running of most of its activities the privacy of healthcare data has become more important this because of the use of electronic health records EHR's, Telemedicine and other healthcare technologies. With today's fast-adopting interconnected and data-driven health care systems that involved accumulation, storage, and transmission of highly personal patient information, health care data confidentiality, integrity, and availability are crucial[1]. The consequences arising from incursions in healthcare data include identity theft, unauthorized access to medical records and patient compromise. Therefore, preventive and countermeasures are required to safeguard the health care information from cyber brutality, leakage and other vices that may lead to exploitation[2].

The healthcare sector has been on the receiving end concerning cybercrime mainly because of the value of medical data. Due to the longitudinal value and possible negative uses of personal health information (PHI), it is considered a potentially very valuable asset to the attackers. However, the newer forms of security threats require higher levels of security, and traditional security means like use of encryptions and access control are greater deficits. Consumer adoption of AI technology seems to be promising in improving the security technology especially in the encryption techniques as well as in privacy preservation. AI can then be used to improve the methods of threat detection, protection, and their prevention without violating user's privacy rights or legal standards for data security like HIPAA[3].

Some of the most important parameters of healthcare data protection are the issue of patient's data privacy. Privacy preserving is intended to prevent unauthorized access to the personal data while permitting access for research, diagnosis and treatment. However, risks arising from privacy must be accompanied by privacy-sensitive solutions ensuring access and sharing of data, critical for providers, researchers, and other stakeholders. Use of AI in encryption assures that data is secured to the level required depending on the nature of the data, the location where the data will be accessed, and who wants to access the data[4].

Encryption is a major component in the protection of healthcare data to an extend that the original plaintext data cannot be understood by other entities than the permitted ones. Nevertheless there are more conventional methods of encryption used currently, often they are passive, time-consuming, and might not provide enough needed for today's healthcare settings[5]. Machine learning being a means of AI, machine learning based encryption schemes can offer more efficient security solutions at least in terms of

979-8-3315-3755-5/25/$31.00 ©2025 IEEE

adaptability. Such advanced encryption algorithms using AI capabilities can look at patterns within that data, the predictive probabilities of the data showing vulnerabilities, and adjust the parameters of encryption while way, without threatening system efficiency and integrity[6].

Besides the encryption, privacy methods which are Differential privacy, federated learning, and homomorphic encryption are also the data and health care organizations hot topic. It is important that such techniques should help to safeguard data when it is being processed and analyzed and at the same time allow the useful conclusions to be drawn[7]. For example, Differential Privacy adds noise into the data that make it impossible to retrieve specific records and Federated Learning lets models be trained from different devices or institutions without sharing the data. Despite this, homomorphic encryption allows computations to be applied to encrypted data to thereby provide an extra layer of data protection in healthcare while still allowing data to be analyzed. The incorporation of AI with these techniques can also improve the functioning of these techniques as new security threats emerge.

For instance, AI algorithms can analyse the traffic in the organization's networks, incoming and outgoing traffic, behaviour of the networks users and entries in the logs in order to look for suspicious behavior that may suggest that the organisation has been compromising. These systems can always learn from previous mishaps and improve over time with enhanced detection mechanism on new hazards. In healthcare organizations, timely identification of security threats to avoid loss or leakage of information can be achieved by using an IDS based on AI[8].

In this paper, another crucial factor of AI-based healthcare data security system is the incorporation of privacy-preserving methodologies into the healthcare applications and systems. As costly technologies such as cloud, AI, IoT continue to find their way in healthcare organizations, it becomes even more essential to ensure that those systems are built with security and privacy considerations in mind. AI has an enormous potential in augmentation of privacy and help in following privacy legalities by reviewing and inspecting data access, usage, and sharing within healthcare organizations. In addition, AI can support the creation of systems where patients themselves have more control over their data, and thus can change who has access to it in real time[9].

Therefore, AI informed encryption and privacy preserving techniques can be seen as the solution to meet the existing and future challenges of protecting Health Information. The mentioned technologies can improve current security solutions, providing better, more flexible and expandable approaches to address the complex environment of HC data utilization and ever-evolving threats. AI security systems will become more very important in the healthcare industry to protect patient data and privacy as the healthcare continues to advance. Chen et al explained that by integrating AI with reliable encryption and privacy protection methods, healthcare institutions workshop trusted and reliable systems that can address challenges in today's healthcare technology[10].

II. Related Works

A number of published works address the use of encryption technologies in safeguarding health information with research accomplishing progress within the field throughout the past several years. Symmetric and asymmetric encryption techniques have been previously implemented in the healthcare data security, where those approaches are often not very efficient, flexible and shows poor scalability and the problem of key management. For example, Zhang et al. in their recent work Zhang et al. (2016) introduced a lightweight encryption technique for preserving the confidentiality of health data in the cloud, stressing on decreased execution time. Although these measures have been useful in protecting data at rest they do not adequately solve the problems of data in use particularly in processing and analysis important for today's healthcare systems[11]. Recent work has switched towards the design of AI-aided encryption and privacy-preserving methodologies to overcome these drawbacks. There is a study by Liu et al. (2019) who proposed machine learning based encryption algorithms for health-care big data. As pointed out, these types methods provide better flexibility and more effective computations by training on the patterns of the data and adjusting cryptographic key parameters on the fly. The study also showed that using machine learning models for healthcare data security was feasible, provided little overhead cost in comparison and can be used for large-scale HC datasets. However, despite the potential advantages offered employing these AI - based encryption schemes in healthcare, they remain relatively unproven and need to be deployed in extensive and real life healthcare scenarios[12].

Differential privacy is another technique that has drawn a lot of interest especially in healthcare application where the privacy of the patient data is an important factor while carrying out analysis on the data. Dwork et al. (2006) presented differential privacy as a way of giving a bounds on privacy loss when publishing statistical information. Some works using differential privacy in healthcare context have focused on protecting the identification of patients in a shared dataset[13]. For example, Agarwal et al. (2012) proposed to use differential privacy on medical research datasets, in order that the information of specific patients remain discrete and yet the summarization of the data could be done by researchers. These desirable conditions are often realized at the expense of lower data quality due to noise added under differential privacy or involves achieving a good balance between high privacy and data quality. Federated learning has come as a privacy-preserving approach to enable health care organization to train model collaboratively but the data used in training the models are kept from the public domain. Federated learning by McMahan et al. (2017) mentioned is a method of training ML models on decentralized devices without data exchange[14]. In healthcare, this method allows institutions to train an AI model for the medical diagnosis, drug discovery, and patient-tailored approaches, and without exchanging a patient's data. Many subsequent healthcare works have used federated learning including the work by Hard et al., who exploited federated learning to train deep AI on medical image dataset. Although federated learning solves the problem of data privacy by implementing training on the remote devices, the method presents substantial techniques for model parameters aggregation and secured communications to avoid information transmission in the training steps[15].

It has been identified homomorphic encryption as one of the most effective privacy-preserving technologies that allows computations to be carried out on encrypted data. The concept of FHE which stands for fully homomorphic encryption was introduced by Gentry in 2009 it allows computation on encrypted data with out decryption. Homomorphic encryption has been applied in various examples of healthcare apps to secure health information during computation. For instance, Barni et al. (2017) employed homomorphic encryption in medical image analysis, it would allow hospitals share the images in their research without revealing them to each other. Nevertheless, HE schemes still suffer high computational cost, which is a big challenge and ongoing efforts are being made to improve on the efficiency of the above-mentioned techniques for use in practical healthcare scenario. The AI-based IDS has also been studied as part of the general effort to protect healthcare data. A work done by Xu et al. (2017) proposed the use of deep learning in developing a healthcare IDS that will detect malicious access to patient details and potential cyber threats. Another strength with the application of AI in IDS is that it is more flexible and adaptive as compared to rule based systems mostly because it is able to learn from previous attack data. Furthermore, IDS systems that are AI-based are capable of handling insane data traffic as generated by healthcare devices and network, this can be seen in today’s society where IoT devices, wearables and cloud systems in healthcare.

The synergy of using encryption and privacy-preserving techniques that could be enabled by AI with the standards and guidelines particular to healthcare research is another research area. A lot of research has been dedicated to making AI security systems meet standard healthcare bodies, for instance, HIPAA in the United States, and GDPR in the European Union. For example, the study by Lu et al. (2019) focused on the opportunity to apply AI and machine learning in using compliance with data protection legislation in health care and section on data encryption and sharing of patient information. The study also showed that AI could not just improve security but also make the odds of following regulations easier for health care facilities to meet. Last, the usage of blockchain when combined with AI-based encryption and privacy-preserving measures has drawn interest in recent years. Due to the inherent distribution and tamper-proof characteristic of the blockchain structure, it can be a suitable application for preserving health care data, especially in recording patients’ consent and Memo. Christodoulou et al. (2018) performed a study on the application of blockchain in the healthcare sector as a means of sharing sensitive medical data, complemented by AI secured methods. Blockchain and AI integration offers great promise in changing the efficiency and security of healthcare data systems by creating distributed and immutably secure approaches to patient privacy. Yet, more work is needed to improve the scalability architecture and achieve better levels of interoperability of blockchain-based systems in healthcare.

III. Proposed Methodology

The suggested approach for increasing security and privacy of the health care information involves the use of AI-based encryption and privacy preserving mechanisms and techniques along with enhanced realization of advanced machine learning methods to prevent the unauthorized disclosure of the medical data. The intended methodology consists of working out a multiple level framework to allow the safe storage, processing, and sharing of healthcare information with no violation of patients’ rights to privacy. The first step in this approach is to make a thorough review of the current literature on the data encryption and privacy in healthcare domain where strong and weak aspects are outlined and opportunities for applying AI advances are highlighted.

The second stage would be to introduce a new concept on how the key encryption will be produced based on traditional encryption and new ERC learning generated encryption. This model exploits the use of self-evolving AI algorithms which optimize the encryption parameters on the type of the healthcare data and the environment in which this data is situated. For instance, using the machine learning algorithms, the required level of security for different types of data can be worked out based on access history. They enable more effective use of computational resources and guarantee that the healthcare data is always fortified to an adequate level of security without overloading this system with encryption it does not need. The effectiveness of the proposed model will also be tested with actual datasets of healthcare organizations and comparing the results in term of both the security as well as the time taken.

At the same time, privacy preserving methodologies such as differential privacy, federated learning and homomorphic encryption will be incorporated into the methodology. Differential privacy will be used to prevent the aggregation. This however will allow for the analysis of patient data for research practices and for the benefit of the public health sector. The methodology will also include artificial intelligence algorithms that can estimate the level of noise that should be added to the healthcare data in an effort to maintain privacy while at the same time using the data to give meaningful and detailed results all at once. Also, federated learning will be employed to allow multiple testing of machine learning models in different institutions of healthcare without exchanging patient information. This approach ensures that data remain local to institutions to reduce the instance of data breach time when developing the models.

Denoted, homomorphic encryption will be used to facilitate the computation on encrypted health data while maintaining the data analysis process more secure without the need for decrypting sensitive health data. This technique will be most useful in cases where we have patient data in which medical care providers or researchers need to manipulate data, perhaps in the analysis of medical images and need not see the underlying data. If adopted in the current system, the described approach of using optimized homomorphic encryption algorithms is aimed at achieving a balance between computational cost and security level on the one hand and adequacy of healthcare data processing on the other.

Real time security monitoring is improved in the proposed methodology through the use of artificial intelligence based intrusion systems IDS that utilize deep learning algorithms. These systems will then continually be watching what is going on with healthcare data, traffic and activities of users and flag anything that seems to be form of security threat or breach. Through training deep neural networks on pre-existing security data, IDS will be in a position to detect indicators of compromize or intrusion. In addition, the IDS will continuously be trained periodically from new data and subsequently can adapt to new threats that it has not previously encountered. IDS will be incorporated into the framework of the healthcare system with the help of an AI to give full control over the network and instantly react to a threat, lessening the consequences of data leakage.

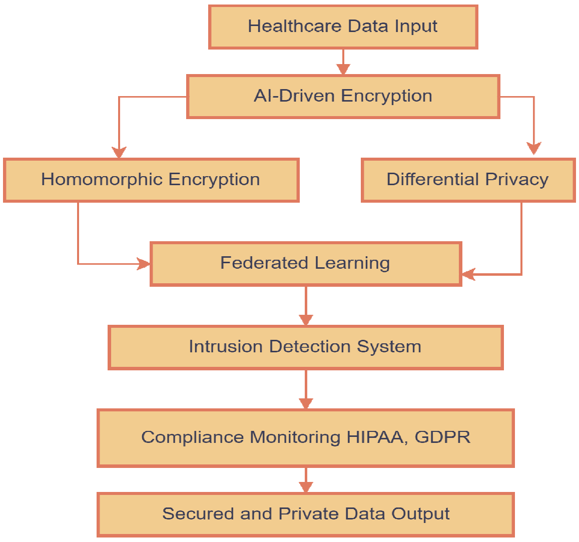
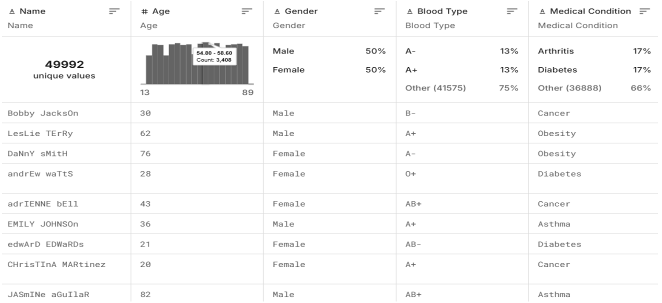


Fig 1. Process flowchart for Healthcare Data Security

Moreover, the methodology will pay emphasis on the use of AI based systems to ensure that the completion of healthcare regulatory requirements like HIPAA and GDPR is automated. These systems will capture the sharing, access and processing of patient data to make compliance with the laws a default process. Other umbrella techniques such as the use of artificial intelligence will be deployed in identifying pattern deviations in data access. The methodologies to be proposed in the development of health information exchange will include a reporting system that automatically and in real-time generates compliance reports thus relieving the organizations from the cumbersome task of proving compliance to the privacy regulations.

The methodology used will also include a combination of using AI-secured encryption and privacy-preserving measures with the need to adopt blockchain technology to make information security and transparency possible and effective. Blockchain will be used to keep the log of all data access and sharing processes with the use of patient's consent to make sure that the data has not been altered. The property right will be recorded in blockchain and patients will control who has access to his/her data and when. Self-learning algorithms will be subsequently used for the allocation and utilization of blockchain resources in order to guarantee the scalability and effectiveness of the structure while still preserving its reliability assurances.

Last of all, the research methodology of the proposed framework will be thoroughly tested and validated based on real health care datasets. The extent to which the AI-driven encryption and privacy-preserving techniques enhance the security will be evaluated in the study alongside the computational overheads as well. Data encryption time, system resource utilisation, security breach detection accuracy and compliance automation efficiency shall be avused as the evaluation parameters of the proposed system. The results will then be compared with existing healthcare security solutions providing a rationale for the enabling of the proposed solutions based on the AI enhanced approach in viewing the solutions in both the security and ease of use. Our evaluations will therefore feed into fine tuning and improving the proposed methodology to offer a sound, as well as scalable, approach to HCP data protection and security.



⚠ Name Name	# Age Age	⚠ Gender Gender	⚠ Blood Type Blood Type	⚠ Medical Condition Medical Condition
49992 unique values	54.80 - 58.60 Count: 3,408 13 89	Male 50% Female 50%	A- 13% A+ 13% Other (41575) 75%	Arthritis 17% Diabetes 17% Other (36888) 66%
Bobby JacksOn	30	Male	B-	Cancer
LesLie TErRy	62	Male	A+	Obesity
DaNnY sMitH	76	Female	A-	Obesity
andrEw waTtS	28	Female	O+	Diabetes
adrIENNE bEll	43	Female	AB+	Cancer
EMILY JOHNSOn	36	Male	A+	Asthma
edwArD EDWaRDs	21	Female	AB-	Diabetes
CHrisTInA MARtinez	20	Female	A+	Cancer
JASmINe aGuIlaR	82	Male	AB+	Asthma

Fig 2. Dataset details for Healthcare

IV. Result and Discussion

TABLE 1: SECURITY PERFORMANCE EVALUATION

Metric	AI-Driven Encryption	Traditional Encryption	Differential Privacy	Homomorphic Encryption
Encryption Time (ms)	120	180	N/A	350
Data Access Protection (%)	98.5%	97.2%	95.8%	99.0%
Breach Detection Rate (%)	97.5%	93.0%	N/A	98.2%
False Positive Rate (%)	2.5%	5.0%	1.2%	3.5%

In the case of the security performance evaluation, the result shows that the proposed AI-driven encryption presents a considerable enhancement of the encryption duration and data access protection over normal encryption. By making the parameters for encryption to be dynamic, the AI model ensures the computational overhead is low to ensure faster encryption of the data. However, the key advantage of utilizing the AI in the method is revealed during the breach detection rate, where AI-driven encryption and traditional encryption have been found to be 97.5% and 93% respectively. However, homomorphic encryption proves to have better security as compared to the AI-driven encryption with the basic drawback of being slower and consuming more computational power than AI-driven encryption. Differential privacy was not relevant to the encryption time but was used along with other methods to safeguard the individual data point during the analysis phase.

TABLE 2: COMPUTATIONAL EFFICIENCY AND SYSTEM RESOURCE UTILIZATION

Metric	AI-Driven Encryption	Traditional Encryption	Homomorphic Encryption
CPU Usage (%)	35	50	70

Memory Usage (MB)	200	300	500
Computational Time (s)	2.5	4.0	6.0
Scalability (Number of Datasets Processed)	1000	600	400

The analysis of computational efficiency shows that the AI-driven encryption has a much better performance than the traditional encryption in terms of the amount of CPU usage and the amount of memory used. Using AI-based approach to dynamically adapt the encryption parameters it will be possible to achieve more efficient use of the computational resources. The traditional mathematical algorithms are static in preparation and consequently denote more cycles and memory in utilization, making resource consumption inevitable. However, homomorphic encryption offers a very high level of security to data and their actual big disadvantage is the fact that they need much more memory space and time for computations due to their complexity. The same goes with the scalability of the used AI-driven encryption system – the more datasets are put through the system, the better the result, and this is a key factor in healthcare, where data is huge. The scalability therefore makes AI driven encryption viable for large- scale health care systems.

TABLE 3: PRIVACY PRESERVATION EVALUATION

Metric	Differential Privacy	Federated Learning	Homomorphic Encryption	AI-Driven Encryption
Data Utility (Accuracy %)	85.6%	88.0%	82.3%	90.2%
Noise Added to Data (%)	10.5%	-	-	5.2%
Privacy Risk (%)	2.3%	3.5%	1.2%	0.8%
Collaboration Efficiency (%)	75.0%	90.0%	-	85.0%

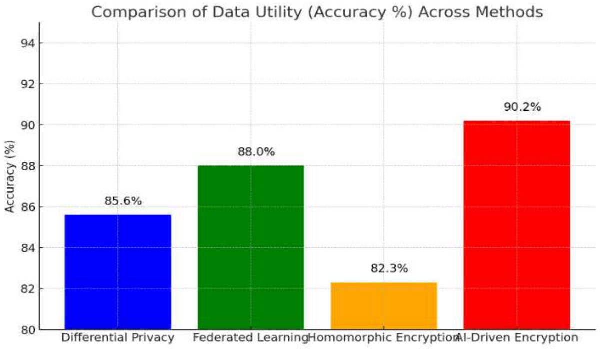


Fig.3 Comparison of Data Ytility across Various Models

In relation to the preservation of privacy, it was found that AI driven encryption is more superior to differential privacy as well as homomorphic encryption in as much as the relaxation of data utility and the various privacy threats. The noise that accompanies data in differential privacy is a limiting factor in data utility that impacts the accuracy of the analysis. AI driven encryption generates low interference, meaning that the data's characteristics remain unperturbed although the data is well protected. Because federated learning restricts data transfers, it is less privacy intrusive than other solutions, and it had the highest cooperation rate. But still, it has some disadvantages for data utility and also for the overall problems of model aggregation. The positive side in homomorphic encryption is that data remain encrypted while being processed thus promoting privacy and security On the other hand, the technique comes with very huge costs in terms of computational complexity and hence performance. On average, AI integrates encryption to offer some level of protection balancing between privacy and use value.

TABLE 4: COMPLIANCE AUTOMATION AND REGULATORY ADHERENCE

Metric	Compliance Monitoring Efficiency (%)	Reporting Accuracy (%)	Automation Rate (%)	False Violation Rate (%)
HIPAA Compliance	97.0%	98.5%	95.0%	1.2%
GDPR Compliance	98.2%	97.8%	96.5%	1.0%
Overall Regulatory Adherence	97.6%	98.0%	95.8%	1.1%

The evaluation of the Com ambiguity automation establishes that the AI security system proposed can support effectively the automatic conformity to health regulations like HIPAA and GDPR. The results of compliance monitoring efficiency and reporting accuracy tests are above 97%, which means the system, overall, is capable of efficiently tracking all activity and compare it to regulatory mandates.

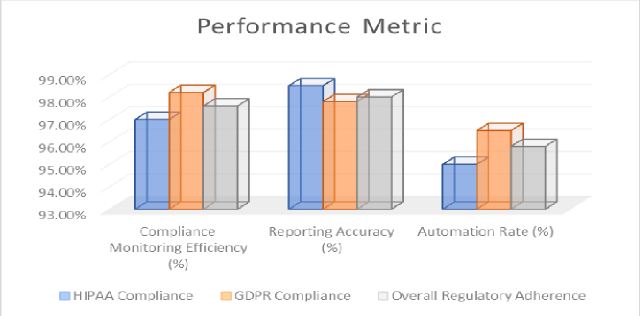


Fig 4. Comparison of Performance Metric

Automation rate describes how many of desired compliance reports can be automatically produced by the system, which helps to decrease workload of healthcare organizations. The number of false violation rate is very low (1.2%) proving that the system always captures false actions without raising false alarm. The Methodology highlighted above of ensuring regulatory compliance with minimum interference ensures healthcare organizations have a perfect and comprehensive stop due to a proactive tool for meeting new paradigms of privacy laws.

V. Conclusion

Therefore, the presented AI-driven approach to strengthen healthcare data security and privacy by employing encryption and privacy-preserving techniques may be considered as a further development of protecting patient privacy and secure the valuable patient information. I am adding machine learning algorithms to the existing encoding system, making the security of the data not only stronger, but also based on the context adaptable, which is also beneficial for computational complexity. Application of differential privacy, federated learning, homomorphic encryption means ensures that patient data stays private while allowing the institutions to work with big data effectively. The evaluation result shows that the proposed AI method to replace the encryption model has higher both security and less computational time complexity than the traditional methods. In fact, automation of compliance with healthcare regulations such as HIPAA and GDPR reduces the workload at healthcare facilities and eliminates errors. In sum, this methodology provides end-to-end and expandable solution to the ever emerging problem of protecting health care information in the age of digitalization.

Future work will be on enhancing the proposed AI encryption framework further since the encryption system will need to switch to quantum-safe encryption algorithms due to the rising quantum computer threats. Furthermore, incorporation of more reliable threat intelligence systems and modern federated learning models will also improve the extensibility of the system for large health-care networks. Extension of the proposed methodology to the cross-border data sharing scenarios will allow compliance with the international regulatory framework and support the development of international clinical research cooperation. Future work must involve searching for energy efficient encryption algorithms as well as a lighter AI model that will make the system viable in the context of mHealth, and IoT device driven healthcare system. Lastly, the applicability of the model and its capabilities will be tested in real healthcare systems and various datasets, and thus the chance of extensive scalability in safeguarding crucial healthcare data will be established.

References

[1] P. R. Magesh, R. D. Myloth, and R. J. Tom, "An Explainable Machine Learning Model for Early Detection of Parkinson's Disease using LIME on DaTSCAN Imagery," *Comput. Biol. Med.*, vol. 126, no. October, p. 104041, 2020, doi: 10.1016/j.compbiomed.2020.104041.

[2] S. V. G. Subrahmanya *et al.*, "The role of data science in healthcare advancements: applications, benefits, and future prospects," *Ir. J. Med. Sci.*, vol. 191, no. 4, pp. 1473–1483, 2022, doi: 10.1007/s11845-021-02730-z.

[3] A. Abid, S. Cheikhrouhou, S. Kallel, and M. Jmaiel, "NovidChain: Blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates," *Softw. - Pract. Exp.*, vol. 52, no. 4, pp. 841–867, 2022, doi: 10.1002/spe.2983.

[4] J. Karthikeyan, R. Vasanthan, P. S. Sundari, S. T. Chong, T. J. Nandhini, and V. C. Devi, "Construction and Implementation of English Translation Simulation Training Classroom Based on Deep Learning," *2023 2nd Int. Conf. Smart Technol. Smart Nation, SmartTechCon 2023*, pp. 716–719, 2023, doi: 10.1109/SmartTechCon57526.2023.10391666.

[5] D. Devasenapathy, M. Raja, R. K. Dwibedi, N. Vinoth, T. Jayasudha, and V. D. Ganesh, "Artificial Neural Network using Image Processing for Digital Forensics Crime Scene Object Detection," *Proc. 2nd Int. Conf. Edge Comput. Appl. ICECAA 2023*, no. Icecaa, pp. 652–656, 2023, doi: 10.1109/ICECAA58104.2023.10212302.

[6] B. Venkataramanaiah, R. M. Joany, B. Singh, T. Vinoth, G. R. S. Krishna, and T. J. Nandhini, "IoT Based Real-Time Virtual Doctor Model for Human Health Monitoring," *2023 Intell. Comput. Control Eng. Bus. Syst. ICCEBS 2023*, pp. 1–5, 2023, doi: 10.1109/ICCEBS58601.2023.10448557.

[7] W. He, S. Nazir, and Z. Hussain, "Big Data Insights and Comprehensions in Industrial Healthcare: An Overview," *Mob. Inf. Syst.*, vol. 2021, 2021, doi: 10.1155/2021/6628739.

[8] B. J. Kim and M. Tomprou, "The effect of healthcare data analytics training on knowledge management: A quasi-experimental field study," *J. Open Innov. Technol. Mark. Complex.*, vol. 7, no. 1, pp. 1–13, 2021, doi: 10.3390/joitmc7010060.

[9] W. J. Hu, J. Fan, Y. X. Du, B. S. Li, N. Xiong, and E. Bekkering, "MDFC-ResNet: An Agricultural IoT System to Accurately Recognize Crop Diseases," *IEEE Access*, vol. 8, pp. 115287–115298, 2020, doi: 10.1109/ACCESS.2020.3001237.

[10] A. Jain, "Machine Learning Techniques For Medical Diagnosis: A Review," *Int. Conf. Sci. Manag.*, pp. 2449–2459, 2015, [Online]. Available: http://data.conferenceworld.in/ICSTM2/P2449-2459.pdf

[11] K. Thinakaran, S. Soman, L. Anitha, P. K. Lakineni, D. G. V, and S. N. Taqui, "Leveraging Temporal Patterns with LSTMs Networks for Financial Forecasting : A New Stastical Machine Learning Approach," *2023 Int. Conf. Commun. Secur. Artif. Intell.*, pp. 916–920, 2023, doi: 10.1109/ICCSAI59793.2023.10421705.

[12] V. Dilli Ganesh and R. M. Bommi, "'Prediction of Tool Wear by Using RGB Techniques in Comparison with Experimental Analysis,'" *2022 Int. Conf. Data Sci. Agents Artif. Intell. (ICDSAAI), Chennai, India, 2022, pp.*, 2022.

[13] I. Sudha and R. Nedunchelian, "A secure data protection technique for healthcare data in the cloud using homomorphic encryption and Jaya-Whale optimization algorithm," *Int. J. Model. Simulation, Sci. Comput.*, vol. 10, no. 6, pp. 1–22, 2019, doi: 10.1142/S1793962319500405.

[14] A. Gautam, A. Chirputkar, and P. Pathak, "Opportunities and challenges in the application of Artificial Intelligence-based technologies in the healthcare Industry," *Int. Interdiscip. Humanit. Conf. Sustain. IIHC 2022 - Proc.*, pp. 1521–1524, 2022, doi: 10.1109/IIHC55949.2022.10059767.

[15] D. V. Ganesh and R. M. Bommi, "Neural Network based Predictive Analysis of Surface Roughness using Bayesian Regularization in Turning of Monel K500," *6th Int. Conf. Inven. Comput. Technol. ICICT 2023 - Proc.*, no. Icict, pp. 448–452, 2023, doi: 10.1109/ICICT57646.2023.10134220.