Strengthening Data Privacy and Security in Modern Healthcare Networks

Gemini A. Parmar[1], Punit C. Trivedi[2]
[1]*Gemini A. Parmar, Atmiya University, Rajkot, Gujarat, India*
[2]*Punit C. Trivedi, Atmiya University, Rajkot, Gujarat, India*

***Abstract*—the ongoing digital evolution of the healthcare sector has resulted in widespread use of connected medical devices, electronic health records (EHRs), cloud-based storage solutions, and advanced data analytics systems. Although these innovations support better patient outcomes, faster diagnostics, and informed clinical decision-making, they also create significant challenges in terms of data privacy and security. Modern healthcare infrastructures are becoming prime targets for cyber threats including ransom ware, information breaches, illicit access, and sophisticated persistent attacks, which pose serious dangers to patient welfare and organizational operations. This review presents an in-depth analysis of current privacy issues and emerging security risks across healthcare networks. It discusses existing regulatory standards, encryption technologies, access control models, intrusion detection systems, the incorporation of blockchain, and the application of artificial intelligence and machine learning in protecting healthcare information. Moreover, the paper identifies weaknesses in present security approaches and recognizes research gaps related to interoperability, protected data exchange, threat detection precision, and regulatory compliance. The study concludes by outlining potential future directions and advocating a multi-layered cyber security framework designed for modern healthcare ecosystems, focusing on system resilience, data confidentiality, scalability, and continuous monitoring to enhance overall security capabilities. Healthcare data security refers to the protection of sensitive medical information from unauthorized access, misuse, or breaches. Emerging solutions leverage** encryption, blockchain, AI, and machine learning **to enhance security and proactively detect potential breaches, aiming to create a trustworthy environment where healthcare providers can safely store, share, and process patient information.**

***Index Terms*—Data Privacy, Healthcare Security, EHRs, Blockchain, Intrusion Detection, Cloud Computing.**

I. INTRODUCTION

The evolution of digital healthcare has significantly changed how medical information is generated, stored, and exchanged within clinical settings [1]. The integration of electronic health records (EHRs), cloud infrastructure, m-health applications, telemedicine platforms, and connected medical devices has enabled quicker diagnosis, personalized care, and better treatment results. These innovations are supported by advanced digital networks that allow smooth data flow between hospitals, diagnostic centres, insurance companies, and patients [2]. At the same time, the growing reliance on digital technologies has increased the exposure of healthcare systems to serious privacy and security risks [3]. Cybercrimes such as ransom ware attacks, data leakage, unauthorized access, and sophisticated persistent threats are becoming more advanced and frequent, targeting confidential patient information and essential medical systems [4]. Since healthcare data is highly sensitive, long-lasting, and valuable, breaches can lead to financial losses, operational disruptions, and damage to reputation [5]. Therefore, safeguarding healthcare data has become a crucial focus for medical organizations and governing bodies. Although existing security solutions like encryption tools, access control policies, and firewall systems provide basic protection, they are often not adequate against new and evolving cyber threats. Advanced security technologies, including artificial intelligence (AI), machine learning (ML), blockchain solutions, and modern intrusion detection systems,

are being explored to strengthen cyber security in healthcare environments.

This review provides an overview of current data privacy practices and security issues in healthcare networks, identifies major weaknesses in the existing infrastructure, and discusses emerging technologies developed to reduce potential risks. It also highlights gaps in research related to secure data exchange, system interoperability, and precision in threat detection. The ultimate goal of this study is to outline a multi-layered security framework suited to the rapidly advancing landscape of healthcare networks. The digital evolution of healthcare has significantly transformed how medical information is managed and used. In recent years, the field has moved rapidly from paper-based documentation to sophisticated digital platforms capable of handling extensive patient datasets [6]. Solutions such as electronic health records (EHRs), virtual healthcare systems, cloud-supported health information platforms, wearable sensors, and the Internet of Medical Things (IoMT) have created an interconnected and intelligent healthcare ecosystem. These technologies support real-time monitoring, remote medical consultations, advanced data analytics, and personalized therapeutic plans, greatly improving patient care and increasing operational efficiency [7].

Despite these advances, the highly integrated nature of modern healthcare networks has introduced new security weaknesses that traditional protection methods cannot fully address. Cyber threats against medical information have surged, with attackers taking advantage of poor authentication controls, vulnerable communication channels, misconfigured cloud repositories, and outdated medical devices lacking built-in security. Rising incidents of ransom ware campaigns, unauthorized access to health data, and widespread information breaches emphasize the immediate need for strong cyber security strategies. Additionally, the high value of medical information on illegal markets—including personal identifiers, genetic profiles, insurance records, and clinical histories—makes healthcare systems a prime target for malicious actors [8]. Global regulatory authorities, including HIPAA in the United States, the GDPR in Europe, and national data protection laws, have developed standards to safeguard patient information and ensure privacy compliance. However, maintaining regulatory compliance while allowing smooth and secure data exchange is a major challenge. Healthcare organizations often struggle to balance interoperability demands with security needs, particularly when integrating new technologies into aging infrastructures. The rapid growth of telemedicine and mobile health applications during the COVID-19 pandemic has expanded the digital attack surface, creating additional risks for healthcare providers and patients alike [9].

To mitigate these threats, modern technologies such as artificial intelligence (AI), machine learning (ML), blockchain, and advanced intrusion detection systems are being incorporated into healthcare defence models. AI and ML support automated threat identification and anomaly detection in real time, while blockchain ensures tamper-proof data storage and decentralized access management. Zero-trust security architecture, strong authentication protocols, holomorphic encryption, and federated learning are emerging as promising approaches for privacy-protected data sharing and collaborative medical research [10].

This review paper provides an in-depth examination of current methods, technologies, and challenges

related to enhancing data privacy and security within digital healthcare networks. It analyses existing security systems, identifies their limitations, and explores innovative solutions capable of defending sensitive medical information against evolving cyber threats [11]. The study also highlights research gaps concerning interoperability, secure collaborative data processing, accurate threat detection, and regulatory compliance in distributed healthcare environments. The primary aim is to propose a comprehensive, multi-layered security architecture that ensures confidentiality, integrity, availability, and traceability while supporting scalable and resilient healthcare infrastructure [12].

II. LITERATURE REVIEW

This study aims to enhance data privacy and security within the Internet of Medical Things (IoMT) by applying Deep Recurrent Neural Networks (DRNN) and machine learning techniques optimized through Particle Swarm Optimization (PSO). The proposed framework accurately identifies cyber-attacks and safeguards sensitive medical information, demonstrating strong performance in intrusion detection to ensure secure and dependable healthcare networks. The hybrid intrusion detection method significantly improves data protection and privacy in IoMT environments by recognizing potential security threats with high accuracy. The research supports the development of reliable and privacy-cantered healthcare systems, and future work intends to incorporate blockchain technology to further strengthen data integrity and transparency in medical infrastructures [1]. The healthcare sector is facing rising concerns related to data privacy and security due to the widespread use of digital medical records and the growing number of data breaches. This discussion emphasizes the importance of biometric authentication in safeguarding patient information and ensuring secure access to healthcare systems. Protecting the confidentiality, integrity, and privacy of patient data within healthcare networks is essential. By integrating biometric security solutions with HIPAA (Health Insurance Portability and Accountability Act) compliance standards, healthcare organizations can enhance data protection, minimize cyber risks, and strengthen patient trust in medical services. In the event of a data breach, it is mandatory to notify regulatory authorities as well as the affected patients [2]. This research examines how Artificial Intelligence (AI) and emerging technologies can strengthen data privacy and security in the healthcare sector. It addresses the challenges created by large-scale medical data, increasing cyber-attacks, and unauthorized access to patient records. The study highlights the use of techniques such as encryption, authentication, and privacy-preserving methods to safeguard sensitive health information. While these advancements enhance patient care and streamline healthcare operations, they also bring notable security risks, such as cyber-attacks, ransom ware, phishing attempts, insider threats, and unauthorized access to electronic health records (EHRs). This research investigates how AI-driven approaches, including machine learning models, anomaly detection techniques, and predictive analytics, can identify and mitigate security breaches in real time.

The paper underscores the importance of secure data management systems to maintain patient confidentiality and build trust in digital healthcare solutions. To ensure the protection of patient data, healthcare organizations must adopt robust mechanisms like encryption, user authentication, and data anonymization. The authors emphasize that enhancing privacy policies, security frameworks, and developing a skilled workforce are critical for the safe and effective use of big data in modern healthcare environments [3]. The study examines key security threats, attack types, and defence techniques in healthcare systems. It highlights the use of machine learning and cryptographic methods—such as Support Vector Machines (SVM), Random Forest, and AES encryption—for intrusion detection and safeguarding medical data. The paper concludes that enhancing security in healthcare networks requires the adoption of structured frameworks like MITRE ATT&CK, along with AI-driven adaptive defence strategies to identify and prevent cyber-attacks. These solutions support the development of a secure, resilient, and privacy-focused healthcare ecosystem [4]. This study introduces a combined approach that integrates process mining techniques with data privacy methods to safeguard confidential healthcare information. Using real surgical unit data from a private hospital, the framework employs anonymization, encryption, and the Fuzzy Miner algorithm to securely analyze and optimize clinical

workflows. The findings show that merging process mining with privacy-preserving practices enhances both system security and the understanding of healthcare processes. The proposed approach enables non-technical users to examine processes more easily while ensuring sensitive medical data remains protected from cyber threats [5]. This paper introduces a risk management framework to protect data privacy and security in Wireless Body Area Network (WBAN) healthcare applications. Since wearable devices continuously collect and transmit sensitive patient data, securing its transmission and storage is essential. The study shows that WBAN systems face significant security risks due to constant data exchange between sensors and medical servers. The proposed framework combines cryptographic methods like AES and Diffie–Hellman with global security standards to ensure confidentiality, integrity, and reliable patient data while meeting healthcare compliance requirements.

If you are using Word use either the Microsoft Equation Editor or the Math Type add-on (http://www.mathtype.com) for equations in your paper (Insert | Object | Create New | Microsoft Equation or Math Type Equation). ―Float over text‖ should not be selected [6]. The paper explains that integrating cryptography with access control helps protect healthcare data stored in the cloud. While cloud systems improve medical services, they also create security and privacy challenges. The study suggests that using strong encryption, access policies, and blockchain technology can secure patient information, making cloud-based healthcare systems safer and more trustworthy [7]. The study highlights key IoT security challenges in healthcare, such as data breaches and authentication failures, and suggests AI can help detect and mitigate cyber threats. Future research should aim to develop integrated AI solutions for secure, reliable, and privacy-preserving healthcare IoT systems [8]. The authors also summarize existing defense mechanisms, such as authentication schemes, encryption methods, and privacy-preserving frameworks, and discuss their limitations. The authors emphasize the need for lightweight, adaptive, and holistic security frameworks that can balance data protection, device performance, and patient safety [9]. Develop a centralized, lightweight cloud-based ML IDS for IoT using a filter-based feature selection, benchmark datasets (UNSW-NB15, KDD Cup 99, NSL-KDD), and comparison of seven supervised ML algorithms [10]. Proposes a stacking ensemble using Logistic Regression, KNN, SVM, and MLP for intrusion detection on the UNSW-NB15 dataset, achieving high accuracy after EDA, preprocessing, and feature selection to classify attacks like DoS, Exploits, Fizzers, and Backdoors [11]. Proposes an IIDPS that detects insider threats by analyzing system-call patterns from user logs with ML classifiers, identifying anomalies by comparing current sequences to learned normal behavior [12]. The proposed system aims to establish a foundation for understanding and demonstrating blockchain applications in various industrial scenarios. For instance, in IBM's industrial blockchain implementation, supply chains are standardized and enhanced based on blockchain principles. This approach is adaptable to multiple sectors, including finance, government, and manufacturing, where safety, scalability, and efficiency are critical [13].

III. METHODOLOGY

The methodologies across the reviewed studies focus on enhancing security, privacy, and threat detection in healthcare IoT networks. Most approaches begin with data collection and preprocessing, using benchmark datasets such as UNSW-NB15, NSL-KDD, and KDD Cup 99, or system call sequences from real user logs to represent normal behavior [1]. Feature selection and engineering are applied to identify the most relevant data points, often using filter-based correlation methods or statistical analysis. For threat detection, machine learning techniques are employed, including supervised models like Logistic Regression, Decision Trees, KNN, SVM, Random Forest, Naive Bayes, and Multi-Layer Perceptron's, while some studies propose ensemble methods such as stacking classifiers to improve accuracy. AI-based intrusion detection systems (IDS) monitor network traffic and system behavior for anomalies, including DoS, Exploits, Backdoors, and insider threats. Privacy-preserving methods, such as anonymization, differential privacy, or federated learning, are integrated to ensure sensitive patient data remains secure. Finally, continuous evaluation, monitoring, and incident response mechanisms are implemented

to maintain network security and reliability in healthcare IoT environments [2].

IV. CHALLENGES AND LIMITATIONS

The reviewed studies on AI-based IoT security in healthcare reveal several key challenges and limitations. Ensuring data privacy and security remains a major concern, as sensitive patient information is vulnerable to breaches and unauthorized access, particularly in networks with weak encryption or authentication [1]. Scalability is another issue, since many AI-based intrusion detection systems require substantial computational resources, making them difficult to deploy on resource-constrained IoT devices [2]. The heterogeneous nature of healthcare IoT environments—with diverse devices, protocols, and data formats—complicates integration and consistent security management [3]. Machine learning models often face limited generalization, performing poorly against novel or sophisticated attacks not present in training datasets, while real-time detection of high-volume IoT data streams remains challenging. Insider threats are difficult to detect due to the complexity of modeling normal user behavior, which can lead to false positives [4]. Privacy-preserving methods, such as differential privacy and federated learning, may reduce model accuracy or increase communication overhead. Furthermore, most studies focus on specific aspects, such as intrusion detection or access control, rather than providing comprehensive, integrated frameworks for holistic security, privacy, and reliability [5]. Finally, AI and ML models require continuous adaptation and retraining to remain effective against evolving cyber threats, adding complexity to system maintenance [6].

V. FUTURE WORK

The future work suggested across the reviewed studies on AI-based IoT security in healthcare emphasizes developing more integrated, robust, and adaptive solutions [1]. Researchers recommend designing holistic frameworks that combine intrusion detection, data privacy, access control, and secure IoT device management to ensure comprehensive protection. There is a need for lightweight AI/ML models that can operate efficiently on resource-constrained IoT devices without compromising accuracy [2]. Future work should also focus on enhancing real-time threat detection and improving model generalization to identify novel and sophisticated cyber-attacks. Privacy-preserving techniques like federated learning and differential privacy need further refinement to balance data protection with model performance. Additionally, continuous monitoring, adaptive learning, and automated incident response mechanisms are suggested to maintain security in dynamic healthcare environments. Finally, large-scale, real-world deployment and validation of proposed frameworks are recommended to address practical challenges and ensure reliability, scalability, and regulatory compliance in modern healthcare networks [3]. Future work for Lightweight Intrusion Detection Systems (L-IDS) for IoT focuses on developing more efficient and adaptive solutions that balance security and resource constraints. Research should explore ultra-lightweight AI/ML algorithms capable of running on low-power IoT devices while maintaining high detection accuracy [4]. Enhancing real-time anomaly detection and improving model generalization to handle new and sophisticated attacks are key priorities. Future studies should also investigate hybrid and ensemble approaches to optimize performance across diverse IoT environments [5]. Additionally, integrating privacy-preserving techniques, such as federated learning or edge-based processing, can protect sensitive data without overloading devices [6]. Finally, extensive real-world deployment and evaluation are needed to ensure scalability, reliability, and practical applicability in heterogeneous IoT networks [7].

VI. CONCLUSION

Improving healthcare data privacy and security requires a multi-layered, technology-driven approach. AI, machine learning, and deep learning models effectively detect cyber-attacks and protect sensitive patient information. Methods like process mining, IoMT frameworks, WBAN risk management, cloud encryption, and blockchain provide strong defenses, while biometric authentication and HIPAA compliance enhance trust. Lightweight solutions, including cloud-based IDS, ensemble models, and IIDPS, offer high accuracy with low resource use.

Overall, an adaptive AI-driven approach, combined with privacy-preserving techniques, is essential, with future work focusing on blockchain and standardized security frameworks to strengthen data integrity and transparency. Hybrid and lightweight security solutions, including cloud-based intrusion detection systems (IDS), stacking ensemble models, and system-call-based anomaly detection (IIDPS), achieve high detection accuracy with minimal resource consumption. Privacy-focused methods like encryption, anonymization, and federated learning protect sensitive medical data while maintaining operational efficiency.

REFERENCES

[1] Saheed, Y. K., & Arowolo, M. O. (2021). Efficient Cyber Attack Detection on the Internet of Medical Things-Smart Environment Based on Deep Recurrent Neural Network and Machine Learning Algorithms. IEEE Access, 9, 161546-161554.

[2] Jayanthilladevi, A., Sangeetha, K., & Balamurugan, E. (2020). Healthcare Biometrics Security and Regulations: Biometrics Data Security and Regulations Governing PHI and HIPAA Act for Patient Privacy. In Proceedings of the 2020 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 12–14 March 2020, pp. 244–247.

[3] Privacy-preserving Artificial Intelligence Techniques in Biomedicine — Torkzadehmahani, R. et al. (2020): a comprehensive survey of AI / ML methods designed to protect sensitive biomedical data while enabling useful analytics.

[4] López-Martínez, A., Gil Pérez, M., & Ruiz-Martínez, A. (2023). A Comprehensive Review of the State-of-the-Art on Security and Privacy Issues in Healthcare. ACM Computing Surveys, 55(12), Article 475 (1–38).

[5] Pacheco Rojas, S., & Armas-Aguirre, J. (2021). Integration method to protect the privacy and security of information in Process Mining projects: A case study on surgery block. In Proceedings of the 2021 IEEE Sciences and Humanities International Research Conference (SHIRCON 2021), Lima, Peru. IEEE.

[6] Paul, P. C., Loane, J., McCaffery, F., & Regan, G. (2021). Towards Design and Development of a Data Security and Privacy Risk Management Framework for WBAN Based Healthcare Applications. Applied System Innovation, 4(4), 76.

[7] Sivan, R. & Zukarnain, Z. A. (2021). Security and Privacy in Cloud-Based E-Health System. Symmetry, 13(5), 742.

[8] Securing Medical IoT Devices: AI-Based Approaches to Vulnerability Management — Kodela, V. (2024).

[9] Newaz, A. K. M. Iqtidar, Sikder, A. K., Rahman, M. A., & Uluagac, A. Selcuk. (2021). A Survey on Security and Privacy Issues in Modern Healthcare Systems: Attacks and Defenses. ACM Transactions on Computing for Healthcare, 2(3), 27:1-27:44.

[10] Divya Priya, A., Kiran, A., & Purushotham, P. (2022). Lightweight Intrusion Detection System (L-IDS) for the Internet of Things. In 2022 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC). IEEE. DOI: 10.1109/assic55218.2022.

[11] V. Santhosh Kumar, S. Saiharish & A. Dinesh Kumar (2024). Network Intrusion Detection Through Stacked Machine Learning Models on UNSW-NB15 Dataset. In Proceedings of the IEEE [conference]. DOI: 10.1109/icses63760.2024.

[12] Utekar, R., & Phapale, A. (2024). Intrusion Detection Systems Using Machine Learning. International Journal of Applied and Advanced Multidisciplinary Research, 2(1), 13–22.

[13] Khatun, M. A., Memon, S. F., Eising, C., & Dhirani, L. L. (2023). Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation. IEEE Access, 11, 145869-145896.

[14] Machine Learning with Deep Learning Approach for Cyber Security Threats Prevention Model. IEEE Conference Publication.