The use of artificial intelligence for the detection of cyber threats in electronic health systems (EHS)

Vesna Simikić[0009-0007-5498-338X]

[1] Faculty of Technical Sciences University of Kragujevac, Svetog Save 65, Čačak, Serbia
simikic.vesna.85@gmail.com

Abstract. Digitization of health systems through the implementation of electronic health systems (EHS) has significantly improved the efficiency and availability of health services, but at the same time increased exposure to sophisticated cyber threats. The application of artificial intelligence (AI) and machine learning (ML) in this context enables advanced anomaly detection and identification of suspicious patterns of user behavior, thereby improving system security. The 2024 and 2025 studies show that models like Isolation Forest, SVM, and EHR-BERT achieve high accuracy in detecting insider threats and unauthorized access in EHS systems. However, the implementation of these technologies faces challenges, including limited access to quality data, false positive alarms, complex IT infrastructure and non-compliance with legislation. Ethical aspects such as transparency of decisions, protection of privacy and responsibility for AI decisions require special attention. Future developments should rely on hybrid models, distributed learning and explainable AI, with standardization of integration into clinical practice. Together, these elements can contribute to a more secure, resilient and ethically responsible digital health infrastructure. AI thus becomes a key tool for strengthening cyber security in modern healthcare.

Keywords: electronic health systems, artificial intelligence, cyber threat, health record

1 Introduction

In recent decades, the digital transformation of healthcare systems has led to the massive integration of electronic health systems (EHS), resulting in improved efficiency, availability and quality of healthcare. However, this digitalization simultaneously opens the door to numerous cyber threats, including unauthorized access, data theft, ransomware attacks, and vulnerabilities in IoT and IoMT devices [6]. The complex interconnection of systems requires sophisticated protection measures that can respond to dynamic threats in real time [4]. In this context, the application of artificial intelligence (AI) and machine learning (ML) is increasingly becoming a key component of modern healthcare cybersecurity [5].

AI and ML offer advanced capabilities for anomaly detection in electronic health records, enabling proactive detection of threats before they cause harm [10]. Models such as EHR-BERT demonstrate high potential in recognizing irregularities and suspicious behavior patterns through complex medical data [9]. The integration of graphical algorithms with machine learning further improves the accuracy and reliability of threat

Research Paper
DOI: https://doi.org/10.46793/BISEC25.273S
Part of ISBN: 978-86-89755-40-4

detection systems in distributed healthcare networks [9]. Such approaches provide healthcare institutions with better resistance to cyber attacks and reduce the risk of losing confidential information.

In addition to progress, numerous challenges continue to hinder the implementation of security solutions in healthcare systems, including the lack of standardized policies, limitations in processing large amounts of data, and complex regulations [11]. Balancing patient privacy and the need for real-time data analysis to prevent incidents is a particular challenge [3]. In addition, mobile health applications and virtual consultations represent additional attack vectors, which requires the development of secure and intelligent architectures such as the CyVHealth system [7]. Continuous research and development of integrated security solutions is needed to respond to evolving threats.

In order to achieve effective cybersecurity in healthcare, it is crucial to establish a multidisciplinary approach that combines technological innovation, regulatory framework and staff education. The role of artificial intelligence is not limited to the detection of threats, but is increasingly used in the prevention and automation of response to incidents [5]. This reduces reaction time and increases the efficiency of security teams. With appropriate technical, organizational and regulatory measures, it is possible to build more resilient healthcare systems that protect both data and patients.

The aim of this paper is to analyze the application of AI for the detection of cyber threats in EHR systems, with special reference to the literature published in international journals in the period 2024-2025. The paper includes the research objective, methodology, literature review, presentation of results through examples of empirical studies, discussion and conclusion with recommendations for practice and further research.

Additional research objectives:

1. Examine how artificial intelligence and machine learning methods are applied to detect cyber threats in EHS systems;
2. Analyze the most significant threats and challenges in digital health systems in the last two years (2024–2025);
3. Show methodological approaches (eg supervised/unsupervised learning, anomaly detection) and their performance in healthcare systems where they are applied;
4. Consider the benefits and limitations of using AI in this context and offer recommendations for future research and implementation.

2 Methodology

For the preparation of this work, a systematic search of professional literature was performed in databases such as Google Scholar, PubMed and ScienceDirect with the following criteria:

- Year of publication: 2024 and 2025.
- Topic: application of AI/ML for cyber threat detection in healthcare, with a special focus on EHR (or electronic health records) and related digital health systems (EHS).
- Type of publication: international journals (peer review).
- Languages: English.

After identifying the relevant articles, an analysis of their methodological approaches, results and conclusions was carried out, as well as a synthesis in review form in the chapter 'Literature review'. Due to the specificity of the topic, empirical studies strictly on EHS systems and AI in the period 2024-2025 are not many - therefore, broader studies concerning digital health systems and threat detection via VA/ML are also included. Implications for EHS systems are also discussed.

3 Literature review

The digitization of healthcare and the introduction of electronic health records (EHR) have significantly improved the efficiency and availability of healthcare services, but at the same time have opened up new challenges in terms of cyber security [3]. The application of AI applications in healthcare systems can increase the risks of breaching privacy and compromising data integrity [1]. In addition, the healthcare sector is increasingly becoming the target of sophisticated cyber-attacks, including ransomware, supplier attacks, and the compromise of IoT/IoMT devices [4].

Due to the growing complexity of threats, there is a need to develop advanced security architectures that integrate artificial intelligence and machine learning for incident detection and prevention [5]. Modern approaches, such as the EHR-BERT model, enable the detection of anomalies in large sets of health data with a high degree of precision [8]. At the same time, it is important to harmonize technological innovations with the regulatory framework that ensures the protection of data and patients' rights [11].

The increasing digitalization of health services and the transition to electronic health systems (EHS) open up new challenges in the field of cyber security, especially in the context of the growing complexity of the digital ecosystem. In the context of smart healthcare, the use of advanced anomaly detection techniques is becoming crucial to identify threats that traditional security systems often cannot detect effectively [2]. An empirical study by Tabassum et al. (2024) shows how a combination of algorithms like Isolation Forest and SVM can achieve exceptional performance in detecting threats in EHR audit logs, with over 99% accuracy. This confirms that anomaly detection methods based on machine learning are of great importance for improving the security of healthcare systems.

In parallel, analysis of threats in mobile health applications provides insight into a wider range of vulnerabilities that threaten EHS and connected devices. Ikegwu et al. (2025) systematically reviewed AI/ML approaches in mobile health and reported that models such as Random Forest, kNN and Naïve Bayes achieve average accuracies between 78% and 84%. Although lower than results in stationary EHS systems, these findings show that mobile applications can also benefit from advanced data-driven analytics. It is important to integrate this knowledge into the overall cyber security strategy of healthcare institutions.

In response to increasingly prominent threats, intelligent architectures are being developed that use machine learning and AI to detect and prevent threats in real time. For example, the CyVHealth architecture offers an approach that combines dynamic data processing, monitoring software, and anomaly detection for protection during virtual

medical consultations [7]. In addition, Niu et al. (2024) developed models like EHR-BERT that effectively recognize patterns of suspicious behavior in networks of hospital records, further confirming the potential of AI in this domain. Technological progress, however, must be accompanied by appropriate regulatory measures to ensure the protection of patients' rights.

The regulatory aspects of implementing AI in healthcare are increasingly coming into the focus of researchers and legislators. According to Virk et al. (2025), it is necessary to harmonize AI solutions with existing laws on data privacy and cyber security in order to preserve user trust and ensure responsible use of technology. Similarly, Al-Suwaidan (2025) warns that inadequate regulation can lead to serious breaches of privacy and data integrity. A comprehensive approach that connects technical innovations with a clear legal framework is the basis for a sustainable and secure digital transformation of healthcare systems.

The application of artificial intelligence (AI) in healthcare systems brings a number of security and ethical challenges, among which the problems of algorithm bias, decision-making without human supervision and potential violation of patient privacy are particularly prominent [2]. These challenges become even more complex when AI solutions are integrated into the complex IT ecosystems of healthcare institutions that include electronic health records, IoT devices and mobile applications [4]. In addition, Al-Suwaidan (2025) warns that not defining responsibility in the event that an AI system makes mistakes can further undermine the trust of users and healthcare professionals.

Additional challenges include limited access to quality datasets due to privacy protection regulations, a high number of false positive alarms during anomaly detection, and the complexity of integrating new AI technologies into existing systems [11]. Also, it is necessary to comply with international standards and laws, such as GDPR and HIPAA, in order to ensure the legal and ethical application of technology [1]. In this context, the creation of a robust regulatory framework and transparent guidelines remains of crucial importance for the sustainable digital transformation of the health sector.

Directing the research focus on electronic health systems (EHS), rather than the broader framework of digital health, allows for a more precise view of specific threats and responses to them. The empirical study of Tabassum et al. (2024) represents a significant example of the application of supervised and unsupervised learning models (IForest + SVM) on EHS audit logs, with an extremely high degree of accuracy. The results of the study indicate that behavioral anomalies of the users, such as activities after the discharge of the patient, are important indicators for the detection of insider threats.

These findings confirm the potential of applying anomaly detection algorithms in real healthcare environments, especially in the context of protecting sensitive medical data. Similarly, Niu et al. (2024) develop models like EHR-BERT and graph-based approaches that enable threat detection in larger hospital networks. These models highlight the importance of contextual analysis and sophisticated AI techniques in improving the security of EHS systems.

Broader reviews indicate that AI/ML techniques are increasingly being applied in mobile health applications and IoT contexts, which opens up opportunities for their application in EHS infrastructure as well [1]. Although these approaches are still in development, they already show significant potential for detecting threats that conventional systems cannot detect. This is confirmed by Hassan et al. (2024), who point out that AI is a key tool in solving the security challenges associated with IoMT devices and a complex healthcare network.

However, it is necessary to take into account the risks brought by the application of AI, including model bias, decisions without human control and challenges in protecting privacy [3]. In addition to technical challenges, there are also regulatory and ethical issues regarding compliance with laws such as GDPR and HIPAA [11]. Therefore, the further development of security solutions must be multidisciplinary, integrating technological innovations with solid normative and ethical foundations.

4 Reasearch results

Analysis of the current literature indicates the high potential of applying artificial intelligence and machine learning (AI/ML) in the detection of threats in electronic health systems (EHS). Anomaly detection algorithms such as Isolation Forest and supervised classifiers such as SVM and Random Forest have proven to be particularly effective. In the study by Tabassum et al. (2024), the combination of IForest and SVM models achieved extremely high results - accuracy of 99.21%, sensitivity of 99.75% and specificity of 99.32%. These results confirm that AI models can reliably recognize suspicious patterns of user behavior within EHS systems.

Similar successes were recorded in mobile health applications, where algorithms such as Random Forest achieved an accuracy of more than 83% [6]. Although lower compared to the EHS context, these results demonstrate the stable performance of the AI model even in dynamic mobile environments. Additionally, research points to the growing importance of IoT and IoMT systems in healthcare, where new threat vectors are emerging that AI can help identify [4]. Hybrid approaches that combine supervised and unsupervised methods are particularly suitable for scenarios with limited labeled data.

A key advantage of unsupervised methods is their ability to detect insider threats, which often go unnoticed by traditional security systems. In this regard, anomalies such as EHS access after patient discharge or unusually long sessions are early indicators of potential abuses [10]. Such data, although technically challenging to analyze, contains valuable patterns of user behavior. The combination of statistical analysis and machine learning algorithms enables their efficient interpretation.

However, the implementation of these solutions faces a number of challenges. Access to large amounts of high-quality and realistic EHS data is often limited due to privacy and ethical norms [11]. Also, the systemic problem of false positive alarms requires additional research in order to reduce the number of false alarms, which can reduce user confidence. Finally, there is a need to standardize the integration of AI solutions into the existing IT frameworks of healthcare institutions [2].

Digital health regulation and policy play a key role in the sustainable development of AI in healthcare. Challenges associated with compliance with laws such as GDPR and HIPAA have been documented, which can limit the amount of data available for model training [11]. At the same time, the literature recognizes the potential of AI to not only improve security, but also support regulatory mechanisms through transparent reporting and oversight [5]. Overall, the analyzes confirm that AI/ML techniques represent a significant resource for improving the cybersecurity of EHS systems, but require careful application while respecting technical, ethical and regulatory frameworks. Based on the research results, I would like to highlight the important fact and emphasize that the United Kingdom, particularly England, is very open to modern approaches to cybersecurity in healthcare systems. The methods I have highlighted are applied at Milton Keynes University Hospital through the implementation of Darktrace AI technology. The public healthcare system in England has positively embraced this, as well as similar AI solutions such as Health Guard, with the aim of detecting potential cyber threats in a timely manner and more effectively protecting patient data. Finally, it can be concluded that the implementation of any new technical solution, including artificial intelligence, requires a well-defined strategy that integrates technical, organizational, and regulatory aspects. Technological efficiency alone is not sufficient without addressing challenges related to data, infrastructure, and the regulatory framework. By developing internationally accepted standards for the safe application of artificial intelligence in EHR systems, AI can become not only a threat detection tool but also a key pillar of modern cybersecurity in healthcare.

5 Discussion

The results of previous research indicate that AI/ML algorithms can successfully recognize threats in EHS systems, especially through the detection of anomalies in user behavior. Identifying activities such as accessing a patient's record after discharge or an unusually long work session has proven useful in identifying potential insider threats [10]. This confirms that highly granular audit logs can serve as a valuable data source for training AI models. However, a key challenge remains in accessing such data due to privacy and regulatory restrictions [11].

Privacy and data availability are among the most significant barriers in the development and evaluation of AI threat detection systems. Many models remain trained on synthetic or partial data, which limits their generalization in real conditions [2]. In addition, the integration of these solutions into complex and heterogeneous IT systems of healthcare institutions represents a technical challenge, especially in the presence of outdated (legacy) systems [4]. These obstacles require standardized interoperability protocols and a strategic approach to introducing AI into clinical practice.

Another important challenge is the control of false positive results. AI systems that are too sensitive can generate a large number of alerts, which can burden healthcare staff and create "alarm ignoring syndrome" [6]. The key lies in striking a balance between sensitivity and specificity, ensuring that only valid threats are flagged [8]. This increases operational efficiency, as well as user trust in technology.

Furthermore, the application of AI in the EHS context cannot be separated from regulatory and ethical issues. Model transparency, accountability for decisions made by AI and fairness in treating users are key dimensions that are often overlooked [3]. In addition, attackers are increasingly using advanced technologies such as generative AI and deepfake, which means that defense mechanisms must also evolve in line with threats [5]. Successful implementation of AI in EHS systems requires not only technical sophistication, but also a concerted strategy that includes staff training, data management, and regulatory compliance.

6 Conclusion

The application of artificial intelligence in the detection of cyber threats within electronic health systems (EHS) shows extremely high performance, especially in the context of detecting anomalies in user behavior. Techniques such as supervised and unsupervised models, including combined approaches, enable timely identification of potential threats, thereby improving system security and patient protection. However, technological efficiency alone is not enough without addressing challenges related to data, infrastructure and regulatory framework.

Key challenges include limited access to quality EHS data, integration into heterogeneous IT systems and the need to reduce false positive results. Additionally, ethical and legal issues—including the transparency, accountability, and fairness of AI systems—require carefully considered standards and policies. Therefore, a strategy that integrates technical, organizational and normative aspects is necessary for the successful application of AI.

Future research should focus on working with real data, developing hybrid models, introducing explainability and applying federated learning in the context of privacy protection. Also, the development of internationally accepted standards for the safe application of AI in EHS systems can contribute to greater trust and wider adoption of these solutions. In this way, artificial intelligence can become not only a threat detection tool, but also a key pillar of modern cybersecurity in healthcare.

Acknowledgments. No acknowledgments.

Disclosure of Interests. I have no interests to disclose.

References

1. Abood, E.W., Yassin, A.A., Abduljabbar, Z.A., Nyangaresi, V.O., Abduljaleel, I.O., Aldarwish, A.J.Y., HNeamah, H.A.Security Challenges and Analysis Tools in Internet of Health Things: A Comprehensive Review. Computers, Materials and Continua. Volume 85. Issue 2. 2025. Pages 2305-2345. ISSN 1546-2218. https://doi.org/10.32604/cmc.2025.066579

2. Admass, W.S., Nunaye, Y.Y., Diro, A.A. Cyber security: State of the art, challenges and future directions. Cyber Security and Applications. Volume 2. 2024. 100031. ISSN 2772-9184. https://doi.org/10.1016./j.csa.2023.100031
3. Al-Suwaidan, F.A. The Security Risks of Artificial Intelligence Applications on the Healthcare System. *Saudi J Health Syst Res* 11 March 2025; 5 (1): 52–54. https://doi.org/10.1159/000542288
4. Hassan, A., Nizam-Uddin, N., Quddus, A., Hassan, S.R., Rehman, A. U., Bharany, S.Navigating IoT Security: Insights into Architecture, Key Security Features, Attacks, Current Challenges and AI-Driven Solutions Shaping the Future of Connectivity. Computers, Materials and Continua. Volume 81. Issue 3.2024.Pages 3499-3559. ISSN 1546-2218. https://doi.org/10.32604/cmc.2024.057877
5. HealthManagement. (2025). AI's Role in Strengthening Healthcare Cybersecurity in 2025. Retrieved from https://healthmanagement.org/c/digital-transformation/News/ais-role-in-strengthening-healthcare-cybersecurity-in-2025
6. Ikegwu, A., Alo, U.R., Nweke, H.F. Cyber threats in mobile healthcare applications: systematic review of enabling technologies, threat models, detection approaches, and future directions. (2025). *Discover Computing*, 28, Article 152. https://doi.org/10.1007/s10791-025-09686-z
7. Manasa, R, Jayanthiladevi, A. CyVHealth: Intelligent Cybersecurity Architecture for Secure Virtual Medical Consultation. Cyber Security and Applications. 2025. 100112. ISSN 2772-9184. https://doi.org/10.1016/j.csa.2025.100112
8. Niu, H., Omitaomu, O.A., Langston, M.A., Olama, M., Ozmen, O., Klasky, H.B., Laurio, A., Ward, M., Nebeker, J. EHR-BERT: A BERT-based model for effective anomaly detection in electronic health records. Journal of Biomedical Informatics. Volume 150. 2024 .104605. ISSN 1532-0464. https://doi.org/10.1016/j.jbi.2024.104605
9. Niu, H., Olufemi A. Omitaomu, O.A., Langston, M.A., Grady, S.K. Olama, M., Ozmen, O. "Anomaly Detection in Electronic Health Records Across Hospital Networks: Integrating Machine Learning With Graph Algorithms," in IEEE Journal of Biomedical and Health Informatics, vol. 29, no. 5, pp. 3723-3735, May 2025, https://doi.org/10.1109/JBHI.2025.3527752
10. Tabassum, M., Mahmood, S., Bukhari, A. et al. Anomaly-based threat detection in smart health using machine learning. BMC Med Inform Decis Mak 24, 347 (2024). https://doi.org/10.1186/s12911-024-02760-4
11. Virk A, Alasmari S, Patel D, Allison K. Digital Health Policy and Cybersecurity Regulations Regarding Artificial Intelligence (AI) Implementation in Healthcare. Cureus. 2025 Mar 16;17(3):e80676. https://doi.org/10.7759/cureus.80676