Cybersecure Healthcare: A Quality Engineering Framework for AI-Driven Patient Safety and Data Protection

Gopinath Kathiresan

Senior Quality Engineering Manager
Independent Researcher, Sunnyvale, USA gopi.385@gmail.com

Abstract

The healthcare sector faces increasing threats from cyberattacks due to the widespread adoption of electronic health records, remote monitoring, and Internet-connected medical devices. This paper discusses the growing role of Artificial Intelligence (AI) in safeguarding critical healthcare infrastructure. AI-driven cybersecurity frameworks are emerging as powerful tools to detect anomalies, identify threats in real-time, and ensure the protection of sensitive patient data. The paper explores the challenges AI systems face, such as false positives, scalability issues, and data privacy concerns, while offering solutions like machine learning, behavioral analytics, and Blockchain integration. A proposed AI-driven framework aims to enhance the security of healthcare systems by providing proactive, real-time threat detection and rapid response mechanisms. Furthermore, the study emphasizes the importance of complying with regulations such as HIPAA, ensuring patient data privacy, and addressing the growing complexity of healthcare networks. Ultimately, AI represents a vital component in securing the future of healthcare cybersecurity.

Keywords: AI-driven Cybersecurity, Patient Data Protection, Internet of Medical Things (IoMT), Data Privacy, Healthcare Infrastructure.

1 Introduction

The healthcare industry is more susceptible to cyberattacks as thousands of clinics and hospitals now use electronic health records, remote monitoring, and medical devices connected via the Internet of Things. Patient information is very sensitive, and healthcare services are essential, which increases the urgency of data breaches. Attacks on key infrastructure like healthcare, energy, and transportation could affect whole economies extremely, and thus, it is an attractive attack target

to have maximum disruption by cyber criminals. Such computer assaults comprise hacking into the system, using ransomware, and shutting down crucial medical services, which all threaten the well-being of patients and hurt the financial status and public image of an institution (Ahmed *et al.*, 2025).

Ransomware cases against hospitals have doubled in recent years. The swift transition to remote working conditions has prompted an increase in cyber-espionage and information holding concerning patient data as a digital form of blackmail, which has led to the lockdown of the entire health system of many locations. This case underscores the fact that the implementation of effective cybersecurity measures that could offset advanced threats is imminent (Neprash *et al.*, 2022).

Intrusion detection technologies based on AI could play an important role in the healthcare IT systems, as such tools can detect unusual patterns of activity and notify the administrator about a possible breach (Savanović *et al.*, 2023). Nonetheless, with the growing number of internet-connected health equipment, referred to as the Internet of Medical Things (IoMT) in general, such systems are generally susceptible to being attacked and need intense protection (Ibrahim, Al-Wadi, and Elhafiz, 2024).

To mitigate this weakness, the monitoring systems based on AI can actively track threats, predicting and intercepting them with the help of sophisticated threat intelligence and indicators of compromise. The AI systems are capable of detecting anomalies through behavioral analysis, unlike the traditional firewall systems, which use static rules. Such systems can handle huge amounts of data and apply machine learning to detect previously unaddressed, hidden threats (Trivedi, Tahir and Isoaho, 2025).

AI in cybersecurity faces numerous issues. These are false positives, data privacy, hazards of adversarial AI attacks, and hazards in the implementation process. Another key challenge is the scalability of huge, distributed networks in health care. The solutions to these challenges are stringent regulatory adherence, policies on data protection, and explainable, interpretable AI models (Achuthan *et al.*, 2024). Moreover, the incorporation of Blockchain technology can take cybersecurity even further by keeping the data authentic, creating tamper-free information, and creating secure audit trails (Almarri and Aljughaiman, 2024).

In this paper, the importance of AI in securing critical infrastructures has been discussed along with the safety implications of securing sensitive healthcare information. The growing incorporation of Artificial Intelligence (AI) in healthcare systems presents numerous opportunities in optimizing patient care, efficiency, and outcomes of treatments. Nevertheless, this also presents serious weaknesses to cyberattacks, and cybersecurity is of great concern. By definition, healthcare entails the preservation and exchange of confidential information, including personal health information (PHI), and such data must be strongly secured. Attacks on medical institutions may have devastating effects, such that data in healthcare, services, and patient safety may be compromised. To overcome such issues, the role of AI cybersecurity frameworks becomes critical in the process of protecting patient information as well as healthcare infrastructure.

2 Literature Review

Cyberattacks on critical infrastructure players have been on the rise in recent years, especially in the case of the healthcare industry. This boom has increased the speed of developing AI-based cybersecurity that allows real-time threat, anomaly detection, and data privacy protection. This section addresses the existing cybersecurity practices, AI use in intrusion detection, and examples of critical infrastructure protection.

2.1 Traditional Cybersecurity Approaches

Conventional approaches to cybersecurity in the healthcare industry include mostly border security tools like firewalls, intrusion detection systems (IDS), and encryption. Such initial methods have been important in protecting health care systems against several cyberattacks. As an example, firewalls check and regulate incoming and outgoing messages so that malicious connections can be avoided, and IDS tools identify unauthorized access and unacknowledged efforts inside networks. With encryption, confidential information such as electronic health records (EHRs) is kept safe when transmitted, thus protecting the patient (Borky and Bradley, 2018).

But these conventional approaches usually fail to handle more advanced and ever-changing cyber threats. Advanced cyber criminals are also taking advantage of newer methods such as ransomware, phishing, and zero-day attacks, none of which can be caught by these security procedures. Most notable is the 2017 WannaCry ransomware, which was aimed at global health organizations, the UK being one of them, via the NHS (WannaCry, 2017). Despite the availability

of firewalls and IDS systems, the system suffered an attack through an unpatched vulnerability of the Windows systems, and this caused mass disruption of healthcare services (Cybercrime, 2023).

Additionally, the healthcare systems become more heterogeneous and integrated, which causes the security boundary to be hard to maintain. The emergence of the Internet of Medical Things (IoMT), connected medical devices, e.g., heart monitors, infusion pumps, and imaging systems, introduces additional vectors of attack to potential attackers. These devices produce real-time data at all times, and they are susceptible to cyberattacks. As a case in point, hackers can use insecure IoT devices in hospitals and use them to tamper with the medical devices, and an example of this is the research on the infusion pumps that identified the vulnerabilities that could manipulate their dose (Hireche, Mansouri, and Pathan, 2022).

Conventional mechanisms of cybersecurity are also failing to deal with the fluidity of healthcare data that changes in real-time due to continuous surveillance and telemedicine. As data flows in and out of medical appliances, through a network, in large quantities containing sensitive information, healthcare systems require more active and dynamic methods of combating new threats. This aspect emphasizes the increasing prevalence of AI-based cybersecurity systems meant to keep up with advanced hacking threats and protect valuable clinical information (He *et al.*, 2021).

2.2 AI Applications in Cybersecurity

The application of AI in cybersecurity has been rising over the last few years, especially in the healthcare sector, where sensitive data regarding patients is vital. With AI-driven solutions, experts introduce new capabilities to the world of cybersecurity that include sophisticated sets of capabilities to detect a threat, discover anomalies, and take immediate action, responding to a cyberattack (Gupta, Kapoor, and Debnath, 2025). The typical approach of humans, in contrast to that of an AI, is that most traditional methods use pre-determined rules and often fail to adapt to changes in the data, which require new rules to be defined. AI systems, on the other hand, especially via machine learning (ML) and deep learning (DL) algorithms, can analyze large volumes of received data used in healthcare networks and devices and learn to show healthy patterns and detect emerging threats. These systems proceed to give a proactive approach to cybersecurity through forecasting probable security exploits through real-time analysis of the stream of data.

The healthcare data, including electronic health records (EHRs), medical imaging, and sensor data, is the other major strength of AI. Such data sources may sometimes have sensitive patient information, so they are hotspots for cybercriminals (Alshehri and Muhammad, 2021). The AI-powered system will be capable of identifying deviations from normative behaviors in real time, including unauthorized access to patient data or strange data interrogation trends. Moreover, AI technology is capable of automatically reacting to identify threats and acting on them by providing protective actions like isolating hacked systems or notifying security personnel, furthermore, decreasing response time and limiting possible harm. Complete automation at this level is especially helpful in the healthcare area, where timely treatment is a priority in ensuring the safety of patients and sustaining the continuity of operations.

2.3 AI in Threat Intelligence and Anomaly Detection

Among the most essential requirements of healthcare cybersecurity, there is an opportunity to recognize and respond to cyber threats before they can become serious instances of healthcare security breaches. Healthcare organizations deal with data that should be kept secret from the patient, and that is why it is a subject to cyberattacks. Its delayed reaction or inability to recognize threats early enough produces a disastrous outcome, such as data loss, interruption of activities, and unfulfilled patient safety. The AI-based cybersecurity has also been quite effective in the detection of anomalies and threat intelligence that allows healthcare organizations to be proactive in detecting the presence of a risk and taking on the shortest time as possible before it can escalate into a big problem.

Through the use of AI-powered systems, all data on a healthcare network will be constantly checked to detect any abnormal patterns or behaviors that might be pointing to an emerging threat. Such anomalies may reflect a variety of cybersecurity concerns, which include malware attacks, unauthorized access, or system weakness. As an example, an AI system may detect an out-of-pattern increase in network traffic by a medical device, indicating a potential malware infection, or in abnormal creation of logins by an unknown IP address, and a restaurant signifying a potential attempt at patient data theft. An early identification of these anomalies enables the AI systems to flag security teams and activate actions to counter possible threats and contain them before they develop (Williams and Woodward, 2015).

Moreover, through new data continuously gathered and updated patterns of threats, the AI models may become more accurate over time, which means that they will better detect and prevent threats as they learn new and more efficient methods of attack. Such a perpetual learning feature enables AI-powered cybersecurity systems to keep pace with an uptick in the sophistication of cybercriminals, who continue to alter their strategies to topple the conventional means of detection.

2.4 Real-world Case Studies in Healthcare Cybersecurity

Several practice case studies can prove the increasing significance of AI-assisted cybersecurity in the healthcare sector. As an example, in 2017, a ransomware attack, WannaCry, interrupted health systems across the globe, including the National Health System (NHS) in the UK (WannaCry, 2017). The attack resulted in the cancellation of appointments, the postponement of surgeries, and the loss of sensitive data concerning patients. Several healthcare institutions realized that more advanced, proactive security was necessary in the resulting fallout.

Machine learning, including anomaly detection systems and predictive analytics systems, has been used to identify malware before it enters the critical systems. These applications study traffic and file patterns in the network to detect suspicious activity that could lead to computer attacks. Moreover, the automation of incident response with the help of AI models is coming in handy to ensure that the cybersecurity teams can concentrate on tackling more complicated incidents, to make sure that the routine threats are automatically addressed.

Table 1 includes a comparison of the key features of the diverse options of AI-based cybersecurity tools, highlighting their distinctive strengths and weaknesses. Anomaly detection and endpoint protection with the assistance of AI have also helped decrease the response time and the number of successful attacks, as well as improve endpoint protection (Bibri, 2018; Alzboon *et al.*, no date). These systems tend to apply unsupervised learning to identify patterns of unusual behavior, which is very effective in identifying threats. Nevertheless, as a weakness, they are likely to produce too many false alarms (Jakubowski *et al.*, 2021)(Alsaig *et al.*, 2019).

Table 1. Comparative Analysis of AI-Driven Cybersecurity Solutions in Critical Infrastructure

Reference	Focus	AI Techniques	Application	Impact	Limitations
(Bibri, 2018)	Traditional IDS Challenges	Rule-based detection	Network security	Effective for known threat detection	Ineffective against novel or advanced

					threats; High false negatives
(Alzboon *et al.*, no date)	AI-Powered Threat Detection	Supervised learning	Intrusion detection in networks	Capable of detecting zero-day and sophisticated threats	Requires extensive labeled data for training
(Jakubowski *et al.*, 2021)	Anomaly Detection Based on Behavior	Unsupervised learning	Real-time anomaly detection	Early identification of previously unknown threats	Tends to generate a high number of false positives
(Alsaig *et al.*, 2019)	Endpoint Security	Reinforcement learning	Device-level threat mitigation	Protects against malware and ransomware	Scalability challenges in large networks

3 AI-Driven Cybersecurity Framework for Critical Infrastructure

Virtual attacks are becoming more innovative and regular, and key infrastructure industries would demand more than conventional protection mechanisms; they would need preventive and multi-tier defense. The presented framework employs automation and artificial intelligence to provide highly developed services in monitoring, preventing, and reacting to constant threats. This allows the identification and mitigation of threats in real time, which can be instrumental in the time-sensitive setting in the healthcare environment, in which continuous operations of the facility and patient safety should be prioritized.

The AI cybersecurity framework, as presented in Fig. 1, is targeted at real-time threat identification and defense capabilities, using anomaly detection, threat blocking, and automatic countermeasure tools to tackle cyber risks effectively. Its well-built architecture offers little room for manipulation by hackers. A sophisticated machine learning-based intrusion detection system (IDS) lies at the core of the system, capable of identifying normal behavior as well as suspicious behavior accurately. In case a threat is identified, the endpoint protection measure is enabled so that it can isolate or kill the threat instantly (Anthi *et al.*, 2019).

When an attack is sustained, the system automatically executes the processes of containment and remediation. Notably, this framework is also intended to align with the currently used security

technologies, including firewalls, Security Information and Event Management (SIEM) tools, as well as access control systems. Such integration improves the overall performance of the existing infrastructures, and this is done by installing dynamic monitoring, adaptive penetrations or controls, and innovative mitigation plans (González-Granadillo, González-Zarzosa, and Diaz, 2021).

This arrangement brings about a flexible and versatile defense mechanism that can protect infrastructure standards. Among them is the fact that it monitors traffic and activities in the network and system continuously to detect anomalies. In contrast to the typical signature-based approaches, which are frequently outraced by zero-day attacks and APTs, AI and machine learning models succeed in detecting obscure, complicated attacks by investigating large quantities of data. After the threat appears, the automated endpoint security blocks the infected device or puts it into quarantine (Ahmed *et al.*, 2025).

The framework will also be based on making the process less labor-intensive, such that response times will be faster and the extent of losses will be smaller. It is anchored on real-time detection of anomalies as well as behavioral analytics, which help detect new threats without being aware of pre-existing signatures. This is implemented through clustering and unsupervised learning, and with the help of behavior profiling of users, devices, and applications. As an example, the system may highlight suspicious items like access to sensitive data regarding patients or a device trying to communicate with unfamiliar services outside the regular working hours.

The next impact is the effective integration of the framework with legacy systems, which allows resolving one of the core issues of moving to a new cybersecurity technology for organizations. It will allow compliance with other regulatory requirements, such as HIPAA and GDPR, providing data security, as well as the opportunity not to violate any legislation through secure security protocols made possible by AI (Nass *et al.*, 2009).

Combining real-time risk identification, anomaly detection, and automatic response measures and SIEM systems dramatically enhances the effectiveness of the framework and its ease-of-use in varying environments. To sum up, the presented AI-enabled cybersecurity framework should enhance the defense of the critical infrastructure by utilizing cutting-edge technologies, persistent observation, and high integration with the current systems to offer an impenetrable shield against modern cyber warfare.

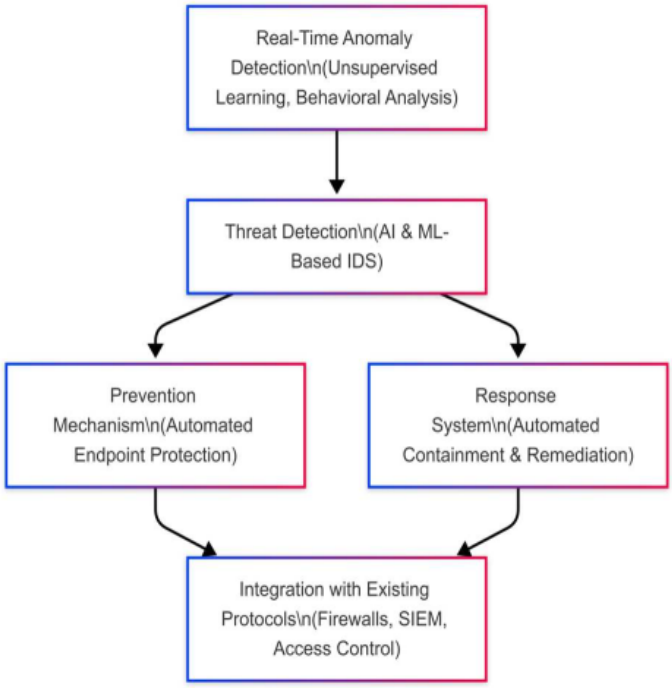

Fig. 1. AI-Driven Cybersecurity Framework for Critical *(Ahmed* et al.*, 2025)*

4 Challenges and Mitigation Strategies

The ability of AI solutions to effectively help address the problem of cybersecurity breaches is another step that makes them more and more attractive than conventional security strategies, especially in such delicate spheres as healthcare. Nonetheless, the implementation of AI-based cybersecurity strategies in critical infrastructure is full of challenges, which may considerably impede the performance and resilience of such systems. Such obstacles encompass the problem of false positive detection, data protection, and scalability of the model, and all these are key to effective and extensive implementation of AI-based cybersecurity solutions (Jimmy, 2023). These are some of the issues that need to be resolved to enable the overall acceptance and adoption of AI solutions in industries, especially those dealing with data that is highly sensitive, like healthcare.

These problems are going to be discussed further in this subsection, along with the possible mitigation measures. Fig. 2 demonstrates the mind map that explains the most remarkable issues connected with AI-based cybersecurity breaches and has a special focus on enterprise information systems. The three key categories of these challenges are listed by the mind map as the adoption of automation that resulted in the diminished experience of foot printing, politically driven cyber

conflicts, and cybercrime. Every challenge is also subdivided into certain issues proposed by the specialists in the area.

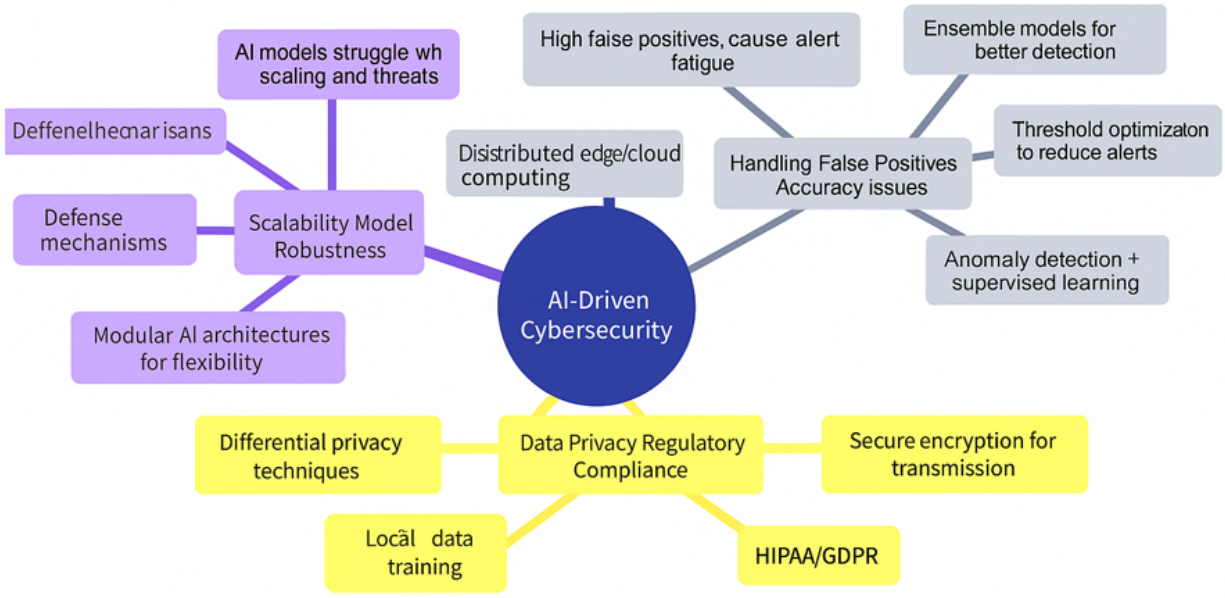

Fig. 2. Mind Map of AI-Driven Cybersecurity Challenges and Mitigation Strategies *(Ahmed* et al.*, 2025)*

4.1 Handling False Positives and Accuracy Issues

The management of false positives may be considered one of the biggest challenges of AI-based cybersecurity. On the one hand, AI models are very effective in recognizing the threat that could happen, but on the other hand, they sometimes create such warnings of non-threatening or non-harmful events. This can cause a high number of false alarms, especially in the healthcare setting where the amount of data is huge and intricate. Security teams need to be sensitive to alerts, but when they become accustomed to hearing numerous false positives, they can end up becoming desensitized to such alerts, raising the chances of missing important threats.

To address this problem, it is extremely important to introduce powerful filtering systems and multi-level validation regimes that can decide what is important and filter out the noise of less important warnings. Such systems must have the capability of distinguishing between high-risk and low-risk incidents to ensure that the security teams shift their attention to the real security breaches. The accuracy of such models can be increased, thereby eliminating the false positives and helping the AI more accurately detect some minor anomalies. Continuous model optimization procedures, testing of the models through rigorous procedures, and calibration to the changing

trends of attacks have to be done to keep the AI algorithms working keenly, accurately, and able to detect any emerging cybersecurity threats in real time.

4.2 Data Privacy and Compliance with Regulations

Special regulations should be meticulously followed by the healthcare organization, such as the Health Insurance Portability and Accountability Act (HIPAA) in the U.S., which ensures the data security of patients (Nass *et al.*, 2009). HIPAA sets a very high bar on how sensitive patient data must be kept secure, and places responsibility on all healthcare providers and the insurance companies to ensure security levels are proper when dealing with their business partners. These involve data privacy, integrity, and availability, as well as avoiding improper ventures of unauthorized access to the health records of patients (Barati *et al.*, 2020). Effective compliance with such regulatory policies and requirements is becoming a necessity as the healthcare industry continues to adopt more AI-based cybersecurity tools. The AI algorithms used to process the healthcare data should be constructed in such a way that protects the privacy of the patient, so that the data that is being processed does not leak any sensitive data.

To address these privacy and security expectations, one can utilize such methods as differential privacy and federated learning. Differential privacy adds some noise to the data in the course of analyzing it in such a way that the data analysis cannot be used to uncover the information about individual patients, but the dataset can still be used to extract useful information from it. The Federated Learning technology, however, enables training AI models on decentralized data depots without the data being moved out of its place. This helps in limiting the chances of data being leaked and makes sure that the data is secured and remains unreachable to other parties as required by regulation. Such sophisticated privacy-preserving methods are necessary to ensure the confidentiality and the trust needed within the healthcare systems, whilst exploiting AI cybersecurity more intensely.

4.3 Scalability and Robustness of AI Models

Cybersecurity systems within healthcare organizations need to change with the volume of data that is being generated by organizations as they expand their operations and even implement cutting-edge technologies. A broad and interconnected digital healthcare environment has been formed due to the implementation of such technologies as Internet of Medical Things (IoMT) systems, electronic health records (EHRs), medical imaging systems, and cloud-based solutions. Such

massive growth in the amount of digital data and connected devices not only makes the network more complex but also adds to the possible points of entry, whereby attackers can target a cyber-attack. To secure healthcare organizations, AI-based cybersecurity systems should scale, be flexible, and be capable of handling the heterogeneous datasets received from various sources (Hireche, Mansouri, and Pathan, 2022).

The AI models should be able to process huge volumes of heterogeneous data, in which they should be able to detect threats, present anomalies across different platforms, including real-time sensor data obtained by medical devices, and large files of medical images. It needs systems that are not only high-performance but also flexible to the emerging technologies, as well as different types of data. It is important to conduct regular stress tests and constant performance analysis to make sure that AI systems will stay productive in a changing environment. To prevent the growing security risks associated with the healthcare network, healthcare cybersecurity systems have to be tested thoroughly to ensure that they are capable of addressing the security issues effectively within the context of the increasing complexity within the healthcare system. The ever-changing threat environment can only be coped with by consistently learning and adapting models.

5 Discussion

The AI-based cybersecurity frameworks represent a revolutionary solution towards the protection of healthcare data and establishing patient safety by offering a real-time and proactive defense against threats. Such frameworks employ cutting-edge AI, including machine learning, anomaly detection, and threat intelligence, to continually scan a healthcare system to identify any possible compromises and attacks. Nevertheless, AI-powered cybersecurity systems face some crucial issues that the solutions have to address to be successfully deployed. Data privacy is one of the most significant issues, and AI systems should be created concerning strict regulations, like HIPAA, and the privacy of patient data should be guaranteed in the course of the analysis and its processing. The false positive problem. Additionally, it is always a challenge to control the false positives; hence, the AI model must be calibrated to detect the true threats and harmless activities to ensure that no security team is saturated with irrelevant alerts. The scalability of the AI models is another burden that healthcare organizations face as they ought to have systems that can process large volumes of diverse data collected by interconnected devices, e.g., IoMT devices, medical records, and image systems.

Additionally, healthcare organizations should also focus on adhering to the applicable regulations, and the AI systems they utilize should be flexible to the ever-changing nature of the threat. Since cyber offenders constantly formulate new strategies and methods of operation, AI models require constant updates and improvements. Last but not least, AI experts, cybersecurity professionals, and regulators should work together with healthcare providers in implementing AI successfully. Through collaboration, these stakeholders will be in a position to create powerful, sustainable cybersecurity systems that will utilize the functionality of AI in threat intelligence, real-time anomaly detection, and quick response to incidents. Such cooperation can greatly increase the potential of healthcare establishments to secure the data of their patients, reduce risks, and respond to new cyber threats.

6 Conclusion

The use of AI-based cybersecurity systems in medicine is not a luxury anymore but a definitive need. Healthcare systems are progressively using digital technologies, and as a result, the amount of sensitive information, including personal health information (PHI), medical records, and current patient data, is rapidly expanding at a scale that has never been seen before. On top of this enormous wave of information, the increasing complexity of cyber-misconduct has rendered former security solutions meant to keep internet waves at bay, like firewalls or simple encryption, hopelessly ineffective in stopping advanced, forward-thinking cyber-attacks. Here, AI can be discussed as an effective tool to strengthen the security of the critical infrastructure, data security of the patient, and patient safety. AI has the potential to identify and eradicate cyber threats in real-time, and using sophisticated machine learning models, it can be proactive compared with real-time prevention through traditional systems.

Nevertheless, to truly achieve its potential in the field of healthcare cybersecurity, AI should also be used to overcome a range of major points of concern, such as the management or false positives, data privacy, the ability to scale to accommodate extreme volumes of varied data, and compatibility with the regulatory environment, such as HIPAA. In combination with the right strategy, AI is capable of automating the process of locating warning signs of a future security compromise, reducing many false alarms, as well as keeping the information of patients secure during all stages of their existence.

With constant innovation, the constant improvement of models, and a capability to react to new threats, artificial intelligence-powered cybersecurity solutions will be central to establishing a resilient health care infrastructure. Not only will these systems ensure the security of sensitive patient information, but they will also take care of the trust and safety of the healthcare institutions and the patients. Neutralizing the threats of cyberattacks, AI may secure the sustainability of healthcare services, facilitate the safe exchange of medical data, and help enhance and improve healthcare delivery quality and efficacy, as a result. The digital healthcare environment is undergoing a form of revolution, and given this dynamism, AI will continue to feature as one of the ways to fight more complex cyber threats and enhance the cybersecurity resilience of global healthcare infrastructure.

7 References

Achuthan, K. *et al.* (2024) 'Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions', *Frontiers in Big Data*, 7, p. 1497535. Available at: https://doi.org/10.3389/fdata.2024.1497535.

Ahmed, N. *et al.* (2025) 'AI-Driven Cyber Security for Safeguarding Critical Infrastructure and Patient Data', in *2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS)*. *2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS)*, Prawet, Thailand: IEEE, pp. 1485–1492. Available at: https://doi.org/10.1109/ICMLAS64557.2025.10968807.

Almarri, S. and Aljughaiman, A. (2024) 'Blockchain Technology for IoT Security and Trust: A Comprehensive SLR', *Sustainability*, 16(23), p. 10177. Available at: https://doi.org/10.3390/su162310177.

Alsaig, A. *et al.* (2019) 'Characterization and Efficient Management of Big Data in IoT-Driven Smart City Development', *Sensors*, 19(11), p. 2430. Available at: https://doi.org/10.3390/s19112430.

Alshehri, F. and Muhammad, G. (2021) 'A Comprehensive Survey of the Internet of Things (IoT) and AI-Based Smart Healthcare', *IEEE Access* [Preprint]. Available at: https://www.semanticscholar.org/paper/A-Comprehensive-Survey-of-the-Internet-of-Things-Alshehri-Muhammad/0caee61694780f17b23883082e2b8038ef55896f (Accessed: 11 September 2023).

Alzboon, M.S. *et al.* (no date) 'The characteristics of the green internet of things and big data in building safer, smarter, and sustainable cities', *International Journal of Engineering* [Preprint].

Anthi, E. *et al.* (2019) 'A Supervised Intrusion Detection System for Smart Home IoT Devices', *IEEE Internet of Things Journal*, 6(5), pp. 9042–9053. Available at: https://doi.org/10.1109/JIOT.2019.2926365.

Barati, M. *et al.* (2020) ‘GDPR Compliance Verification in Internet of Things’, *IEEE Access*, 8, pp. 119697–119709. Available at: https://doi.org/10.1109/ACCESS.2020.3005509.

Bibri, S.E. (2018) ‘The IoT for smart sustainable cities of the future: An analytical framework for sensor-based big data applications for environmental sustainability’, *Sustainable Cities and Society*, 38, pp. 230–253. Available at: https://doi.org/10.1016/j.scs.2017.12.034.

Borky, J.M. and Bradley, T.H. (2018) ‘Protecting Information with Cybersecurity’, *Effective Model-Based Systems Engineering*, p. 345. Available at: https://doi.org/10.1007/978-3-319-95669-5_10.

Cybercrime (2023) *Ransomware, extortion, and the cyber crime ecosystem*. Available at: https://www.ncsc.gov.uk/whitepaper/ransomware-extortion-and-the-cyber-crime-ecosystem (Accessed: 16 June 2025).

González-Granadillo, G., González-Zarzosa, S. and Diaz, R. (2021) ‘Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures’, *Sensors*, 21(14), p. 4759. Available at: https://doi.org/10.3390/s21144759.

Gupta, S., Kapoor, M. and Debnath, S.K. (2025) *Artificial Intelligence-Enabled Security for Healthcare Systems: Safeguarding Patient Data and Improving Services*. Cham: Springer Nature Switzerland. Available at: https://doi.org/10.1007/978-3-031-82810-2.

He, Y. *et al.* (2021) ‘Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review’, *Journal of Medical Internet Research*, 23(4), p. e21747. Available at: https://doi.org/10.2196/21747.

Hireche, R., Mansouri, H. and Pathan, A.-S.K. (2022) ‘Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis’, *Journal of Cybersecurity and Privacy*, 2(3), pp. 640–661. Available at: https://doi.org/10.3390/jcp2030033.

Ibrahim, M., Al-Wadi, A. and Elhafiz, R. (2024) ‘Security Analysis for Smart Healthcare Systems’, *Sensors (Basel, Switzerland)*, 24(11), p. 3375. Available at: https://doi.org/10.3390/s24113375.

Jakubowski, J. *et al.* (2021) ‘Explainable anomaly detection for Hot-rolling industrial process’, in *2021 IEEE 8th International Conference on Data Science and Advanced Analytics (DSAA)*. *2021 IEEE 8th International Conference on Data Science and Advanced Analytics (DSAA)*, Porto, Portugal: IEEE, pp. 1–10. Available at: https://doi.org/10.1109/DSAA53316.2021.9564228.

Jimmy, F. (2023) ‘The Role of Artificial Intelligence in Predicting Cyber Threats’, *International Journal of Scientific Research and Management (IJSRM)*, 11(08), pp. 935–953. Available at: https://doi.org/10.18535/ijsrm/v11i08.ec04.

Nass, S.J. *et al.* (2009) ‘The Value and Importance of Health Information Privacy’, in *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*. National Academies Press (US). Available at: https://www.ncbi.nlm.nih.gov/books/NBK9579/ (Accessed: 23 January 2025).

Neprash, H.T. *et al.* (2022) ‘Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021’, *JAMA Health Forum*, 3(12), p. e224873. Available at: https://doi.org/10.1001/jamahealthforum.2022.4873.

Savanović, N. *et al.* (2023) ‘Intrusion Detection in Healthcare 4.0 Internet of Things Systems via Metaheuristics Optimized Machine Learning’, *Sustainability*, 15(16), p. 12563. Available at: https://doi.org/10.3390/su151612563.

Trivedi, J., Tahir, M. and Isoaho, J. (2025) ‘AI-Enhanced Threat Intelligence in Remote Patient Monitoring Systems: A Survey on Recent Advances, Challenges and Future Research Directions’, *IEEE Access*, pp. 1–1. Available at: https://doi.org/10.1109/ACCESS.2025.3572626.

WannaCry (2017) *WannaCry ransomware attack - Wikipedia*. Available at: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack (Accessed: 16 June 2025).

Williams, P.A. and Woodward, A.J. (2015) ‘Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem’, *Medical Devices (Auckland, N.Z.)*, 8, p. 305. Available at: https://doi.org/10.2147/MDER.S50048.