Received: 17 August 2024 | Revised: 6 March 2025 | Accepted: 7 March 2025 | Published online: 24 March 2025

REVIEW

Medinformatics
2025, Vol. 00(00) 1–11
DOI: 10.47852/bonviewMEDIN52024121

BON VIEW PUBLISHING

Enhancing Cybersecurity Defenses in Healthcare Using AI: A Pivotal Role in Fortifying Digital Health Infrastructure

Shahazad Niwazi Qurashi[1,*], Farrukh Sobia[1], Wafa A. Hetany[1] and Hani Sultan[1]

[1]*Department of Public Health, Jazan University, Saudi Arabia*

Abstract: In the digital health infrastructure, cyber threats pose a long-term security concern for healthcare facilities, and the existing security measures are not capable enough to minimize the risks and security challenges in the healthcare systems. The concept of artificial intelligence (AI) is changing the way healthcare delivery, patient data management, and administrative tasks operate. At present, to elevate threat detection and prevention, we are using key mechanisms like machine learning, Natural language processing (NLP), and other data analytics. With the integrative concept of cybersecurity and generative AI, we can also investigate the impact of AI-driven solutions in healthcare systems. This study emphasizes AI's crucial role in reforming our response to escalating threats and explores the interdependent relationship between generative AI and cybersecurity and their applications in healthcare so that healthcare facilities can predict and mitigate emerging risks by integrating AI into existing security infrastructure. A total of five generative AI-based cybersecurity defense mechanisms are proposed in this study that can be used to enhance digital infrastructure security in healthcare. These five mechanisms represent dynamic strategies that could revolutionize defensive capabilities from real-time anomaly detection to combating zero-day exploits. The suggested technical approaches outline the organizational needs and select appropriate AI technologies and continuous improvement. Fast identification of irregularities and established security standards allow for proactive threat mitigation. Moreover, the proposed strategies ensure proactive threat mitigation and robust security standards for real-time anomaly detection to combat zero-day exploits. Hence, GenAI-based robust cybersecurity protocols are essential to protect digital healthcare facilities from determined cyber opponents.

Keywords: cybersecurity, artificial intelligence, defenses, threats, cyber attacks, healthcare

1. Introduction

To modernize the healthcare systems and with the concern of cyber threats and attacks, most of the countries around the world are focusing on and investing in digital health infrastructure. Digital health infrastructure refers to the integration of digital technologies into healthcare systems. This includes different technologies such as electronic health records, mobile health apps, wearable devices, and health information exchanges. Consequently, a few hospitals are only completely successful in achieving the appropriate health outcomes like improved patient care and enhanced resource data security. But in heterogeneous healthcare systems, to improve the delivery, efficiency, and accessibility of healthcare services and to maintain data confidentiality and integrity, protecting the health system from breaches and unauthorized access is a very big challenge. Lin [1] introduced the applications of AI in various fields of science, namely genomics, drug development, proteomics, transcriptomics, and epigenetics, and promoted healthcare professionals to use artificial intelligence (AI) technology in solving specific biomedical problems.

Unfortunately, many healthcare networks rely on outdated technology and lack the cybersecurity resources and expertise found in other sectors and it makes the healthcare sector vulnerable to cyberattacks. By automating threat detection, identifying vulnerabilities, and incorporating threat intelligence, AI empowers healthcare systems to protect sensitive data and proactively mitigate risks. Many factors such as the adoption of electronic medical records, the rapid proliferation of Internet of Things (IoT) devices, and the effect of the COVID-19 pandemic have expanded the potential attack surface for cyber threats in the healthcare sector. Vukotich [2] concentrated on healthcare and the problems associated with existing cybersecurity measures. As hacking incidents, including ransomware attacks, become increasingly frequent, it is crucial to implement safeguards to protect patient data and the healthcare organization. The instances of breaches were examined, providing insights into their occurrence and potential prevention methods.

With the heterogeneous system environment, hospitals are adopting medical cyber-physical systems (MCPS) to provide continuous, high-quality care to patients, and due to the complexity involved in MCPS, achieving high assurance in system software, interoperability, context-aware intelligence, autonomy, security, privacy, and device certifiability remains challenging. In recent years, generative AI which is a growing technology designed to efficiently generate valuable data holds enormous potential, the GenAI playing a key role in revolutionizing healthcare. Because the computational power is getting more accessible, and health data like electronic health records, electrocardiograms, and medical images are

*Corresponding author: Shahazad Niwazi Qurashi, Department of Public Health, Jazan University, Saudi Arabia. Email: squrashi@jazanu.edu.sa

increasing. Yinka-Yinka-Banjo and Ugot [3] explored various AI-based models to strengthen the concept of cybersecurity in healthcare facilities. Moreover, they emphasized the role of machine learning models including GANs in identifying and mitigating cyber threats. Such models also ensure the confidentiality and integrity of healthcare data.

Therefore, ethical and transparency concerns and related issues have arisen regarding the potential aggravation of health inequalities due to the improper use and implementation of this technology in healthcare. Moreover, from the research point of view, medical professionals and researchers are keeping more focused on the generative AI concept and its applications which has gathered significant attention, sparking debates about its scope in healthcare. Outdated systems pose extensive threats and associated risks. Recognizing and addressing these threats is crucial for maintaining security across the healthcare environment. Analyzing threats and vulnerabilities provides an effective approach to mitigating the risks associated with these vulnerabilities. The latest generative AI-based security mechanisms are the necessity to implement in the healthcare system to overcome the existing problems. In the study, a few security defense mechanisms are discussed including their use cases and required their action plans. Overall, the existing capacity of security measures is quite inadequate to reduce the risks and address security challenges in healthcare facilities. This research gap highlights the need to identify and develop innovative AI solutions that will be tailored to the unique cybersecurity requirements and needs. In the healthcare sector, outdated systems face extensive security threats and risks, and hence, recognizing and addressing these threats is a vital need to maintain security across healthcare settings. The objective of the study is to propose an effective set of strategies and AI-based security mechanisms. Moreover, the study aims to demonstrate the effectiveness of generative AI technologies and security mechanisms in improving the security of healthcare environments.

2. Related Work

Inkster et al. [4] studied the existing condition of cybersecurity in the digital mental health sector to jointly pinpoint risks and safeguard the vulnerabilities of users and providers and proposed the formation of a cybersecurity culture within digital mental health. Yeng et al. [5] conducted a study to identify suitable AI techniques and data sources for effective modeling and analysis of healthcare staff's security practices. They developed and implemented a framework using simulated data, offering a holistic method for modeling and analyzing the security practices of healthcare staff using real access logs. Arshad et al. [6] investigated bio-cybersecurity threats related to genomic-DNA data and software applications that utilize such data for scientific research. Using empirical methods, they analyzed and identified vulnerabilities within genomic-DNA databases and bioinformatics software, aiming to prevent cyberattacks that could compromise the confidentiality, integrity, and availability of this critical data.

Roosan et al. [7] proposed a conceptual framework based on blockchain and AI by conducting a scoping review of successful blockchain integrations in health systems to enhance access to healthcare data in the community pharmacy setting through the adoption of blockchain technology and AI. They used the Pharmacists' Patient Care Process to pinpoint crucial areas for blockchain integration that can assist community pharmacists in accessing patient's electronic health records and incorporating patient-specific information into clinical decision-making. Almaiah et al. [8] introduced a two-layer blockchain-based deep-learning framework in which a blockchain scheme was proposed where each participant was registered, verified, and subsequently validated using an enhanced Proof of Work based on smart contracts to achieve security and privacy. Using a variational auto-encoder technique, a deep-learning scheme was also designed for privacy and a bidirectional long short-term memory or intrusion detection. Nayak et al. [9] introduced a new IoMT framework combining Bayesian optimization and an extreme learning machine that showed promising results and improved decision-making accuracy compared to other contemporary methods.

Salim and Park [10] used a decentralized Federated Learning-based Convolutional Neural Network model to train data locally within the hospital and store the results in a private Interplanetary File System, and the evaluation results showed that in terms of accuracy, sensitivity, and specificity, the decentralized CNN model performs almost the same as the traditional centralized model. Ramasamy et al. [11] developed an AI-powered Internet of Things Cyber-Physical System intended for physicians to diagnose various medical conditions in patients to detect diseases such as diabetes, heart disease, and gait abnormalities. Wahab et al. [12] proposed an AI-powered, SDN-enabled Intrusion Detection System for e-health and IoMT environments. Combined LSTM and GRU models, evaluated using the CIC DDoS 2019 dataset, achieved high-performance metrics such as 99.01% accuracy and 99.12% $F1$ score. Ali et al. [13] emphasized the significance of Federated Learning within IoMT networks to uphold privacy and introduced advanced Federated Learning structures incorporating Deep Reinforcement Learning, Digital Twin, and GANs to identify privacy vulnerabilities. Radanliev et al. [14] investigated cybersecurity risks in the context of AI and technological singularity and developed a framework to mitigate AI-related risks, emphasizing the importance of AI in defense and preventing autonomous AI device actions. Biasin and Kamenjašević [15] examined the interaction between new reforms and existing laws from a cybersecurity perspective and found that simultaneous implementation of similar measures could lead to fragmentation and inconsistent protection levels in healthcare.

Horowitz et al. [16] studied the influence of human inclinations on the adoption of AI-powered autonomous technologies and found that individuals with AI knowledge were more inclined to endorse autonomous applications across various fields compared to those with limited understanding. Kelly et al. [17] proposed cybersecurity principles for medical imaging, detailing strategies for detection and prevention, and the role of technology in enhancing security and offered suggestions for radiologists to understand threats linked with radiology AI. Oniani et al. [18] investigated ethical principles for generative AI in healthcare from a military perspective and presented a framework for implementing ethical principles such as Governability, Reliability, Equity, Accountability, Traceability, Privacy, Lawfulness, Empathy, and Autonomy. Riggs et al. [19] compiled significant cyber data to examine types of cyberattacks, their impacts, vulnerabilities, and the victims and perpetrators and cataloged cybersecurity standards and tools to tackle these issues. To safeguard the integrity of sensitive healthcare data in AI-driven medical research, Barbaria et al. [20] proposed a blockchain-based architectural framework and conducted a comprehensive analysis of public administration purchase records for potentially vulnerable medical devices.

Selvarajan and Mouratidis [21] introduced a technique for secure data exchange within healthcare systems using blockchain technology and shaped a distinctive key pair for secure storage of patient data in hash value blocks. Cartwright [22] described on the daily use of IoMT devices in anesthesia and ICU, highlighting the

potential entry points for cyber threats and the risks to patient safety and PHI, and also emphasized the need for secure IoT devices in healthcare.

Silvestri et al. [23] applied machine learning models like BERT and XGBoost to analyze threats and vulnerabilities in healthcare and extracted information from natural language documents to assess the severity of threats and provide effective risk management. Rubinic et al. [24] investigated the misuse of large language models in clinical pharmacology for creating bioweapons and proposed mitigation strategies including explainable AI, ethical guidelines, and policy deviations to address ethical issues.

Messinis et al. [25] studied contemporary cybersecurity technologies using AI methods and emphasized that machine learning and deep learning enhance the performance, speed, reliability, and effectiveness of cybersecurity measures, especially in IoMT. Zhan et al. [26] identified obstacles to adopting digital information systems in healthcare and highlighted that outward attacks and technological factors were the main challenges, while employee-related factors had a lesser impact on the adoption process.

Supplementary Table 1 summarizes the comprehensive description of the previous research work conducted in the field of GenAI and cybersecurity, highlighting the key advancements specifically the Pros, Cons, and Prediction Techniques used. It is attached as a supplementary file.

3. Current Scenario of Cybersecurity and GenAI in Healthcare

The integration of generative AI is transforming the healthcare field by offering advanced patient care, administrative efficiency, and clinical productivity. At the same time, due to the heterogeneous environment, healthcare systems are interconnecting and increasingly vulnerable to cyberattacks. With the immense potential of GenAI to revolutionize healthcare, and for addressing the associated cybersecurity risks, there is a huge requirement to integrate and to deploy combined concepts. For example, MCPS are an application of AI in healthcare that helps us to explore various applications of CPS-based healthcare systems like telehealth for chronic disease management and tele-homecare systems. MCPS are being gradually adopted by hospitals to deliver continuous, high-quality care to patients. The MCPS represents a networked system of medical devices that are life-critical and context-aware.

Shaikh et al. [27] detailed the four levels of MCPS architecture viz. data collection, aggregation, cloud processing, and action. They focused on the use of varied encryption methods across layers to maintain data privacy amidst hardware differences. This research also compared old and newer encryption techniques regarding secure data handling. Results showed that while advanced encryption enables innovative features, it heightens computational and storage demands. Secondly, advances in AI technology raise concerns about ethical, moral, and legal safeguards, necessitating immediate improvement in evaluating security, privacy, and ethical management. To tackle these issues, Mylrea and Robinson [28] introduced an AI Trust Framework and Maturity models aimed at enhancing confidence in both the design and operation of AI systems.

4. Implementation Requirements for Cybersecurity

The list of implementation requirements is given in Figure 1 to enhance clinical decision-making, optimize treatment strategies, and streamline resource allocation, and there are several key technical and ethical requirements for integrating AI and cybersecurity within healthcare facilities. AI systems should be designed to protect sensitive medical data from cyber threats. The ethical implications of AI in healthcare need to be thoroughly considered, and strategies to protect against cyber threats should be carefully

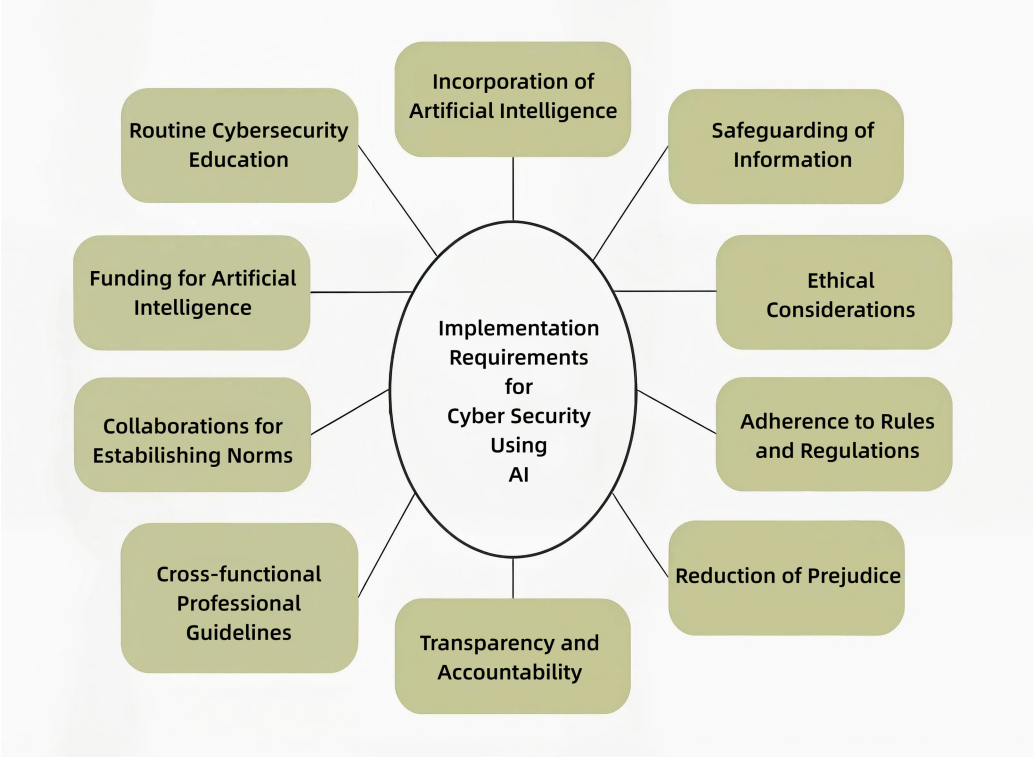

Figure 1. Implementation requirements

implemented, and systems must comply with all relevant laws and regulations.

AI-based systems should adhere to the principles of transparency, accountability, and safety, ensuring they are transparent and accountable and the regulations that govern them continue to evolve, there is an increasing need for multi-disciplinary industry standards. Organizations should work together to establish guidelines and industry standards to promote responsible implementation of AI in healthcare and regular training can help staff recognize and avoid potential threats, such as phishing attempts.

5. Generative AI in Healthcare Administrative Procedures and Cybersecurity

Before AI implementation, it is essential to assess the capabilities and constraints of the healthcare systems. Ensuring extensive, representative, and unbiased training data is vital for AI algorithms. Generative AI can transform administrative procedures using automating tasks and improving efficiency in healthcare and also simplify drafting administrative documents by generating coherent and well-structured texts through automating documentation, streamlining administrative tasks, and enhancing data analysis. Generative AI enhances cybersecurity by predicting and managing threats proactively. By learning from historical data, GenAI identifies patterns in cyber threats and vulnerabilities, enabling anticipation of future threats. It aids threat hunters with data retrieval and offers real-time insights for vulnerability management, improving efficiency, security, and decision-making.

6. The Proposed AI-Based Cybersecurity Defenses and Mechanisms for Healthcare Facilities

By leveraging AI, healthcare facilities can significantly enhance their security bearing, protect sensitive patient data, and ensure the smooth operation of digital health systems. The proposed AI-based cybersecurity defenses and mechanisms model is a premeditated model, and the security mechanisms can be utilized step by step. The cybersecurity defenses and mechanisms are given in Figure 2.

6.1. Integrating generative AI into security tool administrative interfaces

Integrating the generative AI into the administrative interface is highly required as it can create new data or content based on existing data or models. It can also create text, images, audio, code, and other forms of data, employing methods like deep learning, natural language processing, computer vision, and generative adversarial networks. Overall, generative AI provides solutions for improving diagnosis, treatment, prevention, compliance, and risk management. Apart from this, generative AI also poses some risks and challenges, such as ethical, legal, and technical issues, that need to be addressed and mitigated.

In this context, we explored and proposed how generative AI can be integrated into security tool healthcare administrative interfaces, and how it can be supportive for actions like researching cyber adversaries, understanding attack paths, generating compliance reports, customizing security policies, and quantifying security risks in Figure 3(A) and (B).

Action 1: Researching Cyber Adversaries

Cyber adversaries are malicious performers who seek to compromise, damage, or steal data or resources from healthcare systems, devices, or organizations. Generative AI can play a key role in researching cyber adversaries in the healthcare system by collecting, analyzing, and modeling cyber threat intelligence from various sources, such as network traffic, intrusion alerts, threat reports, and open-source data. The use cases of generative AI for researching cyber adversaries are given in Table 1.

Action 2: Understanding Attack Paths

Attack paths are the sequences of steps or vulnerabilities that cyber adversaries exploit to compromise a target system, device, or organization. These paths consist of three components, i.e., an asset of a given value, a threat to the integrity and safety of that asset, and the potential impact of that threat. Understanding attack paths is important for assessing and mitigating the cyber risks and impacts in healthcare. The healthcare systems and medical IoT devices often store, process, and transmit sensitive and critical

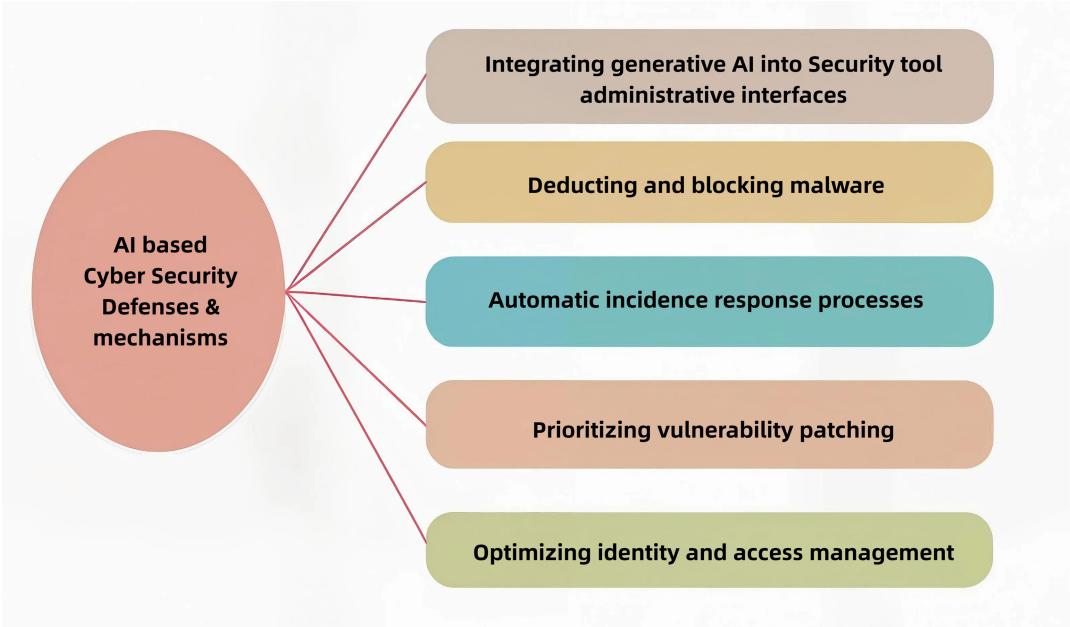

Figure 2. Cybersecurity defenses and mechanisms

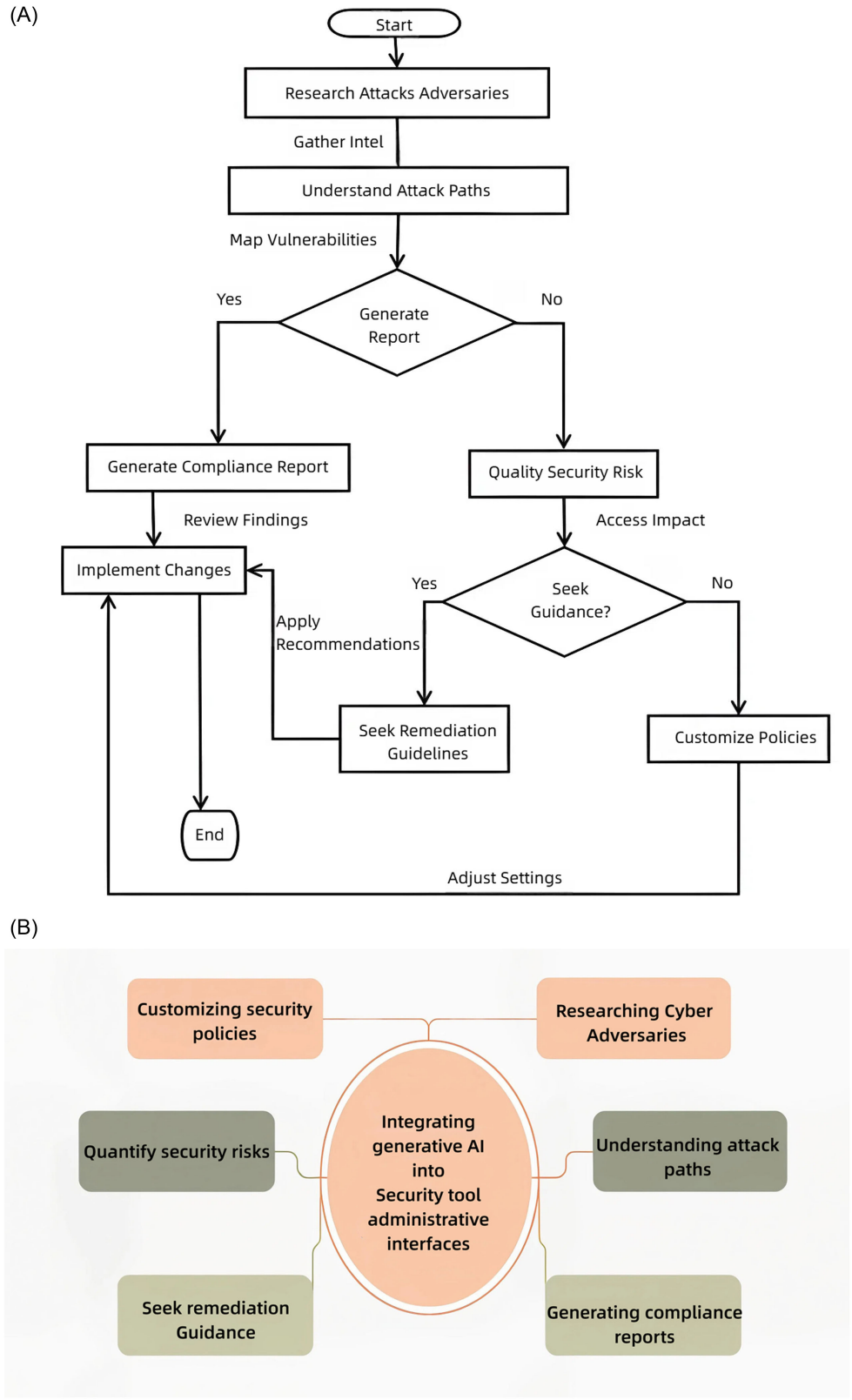

Figure 3. (A) Flow chart representing the implementation of integrating generative AI mechanisms. (B) Integrating generative AI mechanisms

Table 1. Use cases of generative AI for researching cyber adversaries

	Use cases
1.	Generating realistic phishing emails or websites – based on the target's profile and preferences
2.	Creating synthetic malware samples or variants – based on known or unknown malware families
3.	Modeling the attack paths and strategies – based on their objectives and resources
4.	Predicting future actions and trends – based on historical and current data

data and resources. To understand attack paths by identifying, visualizing, and prioritizing the attack paths in a healthcare environment, we can use the concept of generative AI and it can also use optimization and decision-making techniques to rank and score the attack paths based on their likelihood, severity, and cost and to suggest the best mitigation actions or strategies. In this case, we can consider the following use cases of generative AI for understanding attack paths mentioned in Table 2.

Table 2. Use cases of generative AI for understanding attack paths

	Use case
1.	Generating Attack Graphs or Trees – Show possible attack paths from entry points to assets Examples: medical IoT devices, patient records, networks
2.	Visualizing Attack Paths – Interactive and intuitive visualizations Formats: graphs, charts, maps – Highlight key vulnerabilities, exposures, impacts
3.	Prioritizing Attack Paths – Based on risk scores Factors: asset value, threat probability, impact
4.	Recommending Mitigation Actions – Optimal strategies for each attack path Examples: patching, encrypting, isolating, monitoring

Action 3: Generating Compliance Reports

Generating compliance reports is important for maintaining and improving the performance and reputation and to avoid penalties, fines, or lawsuits for non-compliance. Generating compliance reports is also challenging because compliance requirements are complex, and compliance data are often scattered, incomplete, or inconsistent. Use cases of generative AI for generating compliance reports are specified below in Table 3.

Table 3. Use cases of generative AI for generating compliance reports

	Use case
1.	Creating compliance reports – To summarize the compliance status, findings, and recommendations of a healthcare system Compliance requirements: specific rules, standards, or regulations.
2.	Formatting compliance reports – To present the compliance data clearly and concisely, using tables, charts, or graphs
3.	Updating compliance reports periodically or on-demand, based on the changes in the compliance requirements or data

Action 4: Quantify security risks

In the healthcare industry, we need to quantify security risks to assess and measure potential threats to patient data, system integrity, and overall safety. Overall quantification involves measuring risk aspects precisely, and effective risk management involves continuous monitoring, mitigation, and informed decision-making.

Action 5: Seek Remediation Guidance

To recommend remediation guidance for security risks, generative AI prioritizes risks based on severity and likelihood and consequently restricts entry to confidential data and systems. It secures data with encryption while stored and during transmission by using strong authentication methods.

Generative AI uses antivirus software and endpoint security solutions, develops a comprehensive incident response plan, complies with relevant healthcare regulations, and updates software and systems to fix recognized vulnerabilities. Apart from this, it splits critical systems from less secure environments and monitors network traffic for any suspicious activity.

Action 6: Customizing security policies

Security policies take place for implementing and enforcing security measures like authentication, authorization, encryption, monitoring, and auditing, that aim to protect the confidentiality, integrity, and availability of the system, device, or organization. For a particular situation, generative AI can help with customizing security policies by designing, testing, and optimizing the security policies based on the security needs, preferences, and constraints of the system, device, or organization. To design security policies, generative AI uses machine learning and optimization that meet the security objectives, principles, and procedures of the system, device, or organization and also comply with the relevant rules, standards, or regulations. Simulation and evaluation are also the procedures to test the security policies against various scenarios, such as normal or abnormal operations, and expected or unexpected events.

6.2. Deducting and blocking malware in the healthcare system

Malware or malicious software poses a serious threat to the healthcare system, as it has the potential to challenge the secrecy, accuracy, and accessibility of sensitive information and critical data and resources, such as patient records, medical devices, or hospital networks. Some methods and tools for deducting and blocking malware in healthcare systems are antivirus software, firewalls, sandboxes, and honeypots. Table 4 summarizes the actions for deducting and blocking malware.

6.3. Automatic incidence response processes in healthcare facilities

Challenges and Requirements of Automatic Incidence Response Mechanism

1) Complying with the relevant regulations and standards
2) Protecting sensitive and critical data for example: patient records, medical devices, or hospital networks
3) Coordinating the diverse and dynamic stakeholders, such as healthcare providers, patients, and regulators.

The automatic incident response can be utilized as a defense in healthcare to accomplish various tasks as described in Table 5.

Table 4. The use cases for deducting and blocking of malware

Actions	Applications
Static File Analysis	To extract valuable information or identify malicious behavior using Various methods and tools, like file type identification, format analysis, metadata extraction, code disassembly, decompilation, code analysis, and machine learning.
Anomaly detection	Detecting fraud, intrusion, faults, monitoring systems, or diagnosing issues within systems using statistical methods, deep learning, clustering, classification, regression, isolation forest, and Python
Behavior analysis	Measuring and comprehending the actions, reactions, and interactions of individuals, groups, or systems using methods and tools in healthcare setups like observation, experimentation, surveys, interviews, questionnaires, social network analysis, and sentiment analysis.

Table 5. Automatic incident response can be employed as a defense in healthcare to achieve the following tasks

Task to achieve	Required automation tools and techniques	Use cases /Implementation
Security event validation and prioritization	Rule-based logic, ML, and AI,	**Using data integration and correlation** -Consolidate and cross-reference the security events from different sources, like antivirus, firewall, sandbox -Identify the common or related events, like the same source, target, or type of incident. **Using machine learning or artificial intelligence** -Validate and prioritize the security events based on their features, patterns, or anomalies
Identifying and isolating infected systems	Network monitoring, Endpoint detection, and Threat Hunting	**Using network monitoring** -Detect and identify the infected systems, devices, or networks based on the network traffic, such as the source, destination, protocol, or payload, and -Flag or alert the suspicious or anomalous traffic, such as traffic to or malicious domains, IP addresses, or ports **Using quarantine** -Isolate the infected systems, devices, or networks from the rest of the healthcare system using a virtual machine
Notifying users of compromised devices	Changing passwords, updating software, or Contacting support	**Using email, SMS, phone call, or push notification** -Send or deliver notification messages to the users of the compromised devices, and -Provide the relevant information or instructions, such as the nature, scope, or impact of the cyber incidents, tips, or resources to cope with the cyber incidents **Using a chatbot, voice assistant, or web portal,** -Interact or communicate with the users of the compromised devices, and -Answer questions or concerns, or offer assistance, that the users may have regarding the cyber incidents.
Blocking suspicious IP addresses	Threat intelligence, ML, or AI	**Using threat intelligence** -Identify and classify suspicious IP addresses based on their characteristics, behavior, or reputation. -Refine the blocking rules or policies based on the changes in the threat environment. **Using a firewall** -Block or limit the inbound or outbound traffic to or from the suspicious IP addresses, and -Restrict or control access to or from suspicious IP addresses.
Revoking access credentials	Identity and access management, Multi-factor authentication, or password reset	**Using identity protection** -Identify and classify the access credentials based on their characteristics, behavior, or reputation. **Using machine learning or artificial intelligence** -Identify and classify the access credentials based on their features, patterns, or anomalies

6.4. Prioritizing vulnerability patching

6.4.1. Using CVSS score and accessibility via the Internet

Prioritizing vulnerability patching based on CVSS (Common Vulnerability Scoring System) score and accessibility via the internet is a method that helps to rank and schedule the patches or updates for the vulnerabilities, based on the combination of their severity and exposure and to focus on the most critical and urgent vulnerabilities that pose the highest threat to the healthcare system. This mechanism can prevent or mitigate cyber threats from accessing or compromising the healthcare system and protect sensitive and critical data and resources, such as patient records, medical devices, or hospital networks.

This mechanism applies to the following use cases:

1) Using a matrix or a formula to calculate the priority of a vulnerability patching based on the CVSS score and accessibility via the internet, such as using the following formula:

$$\mathbf{Priority} = \mathbf{CVSSscore} * \mathbf{Accessibilityfactor},$$

where the accessibility factor is a value between 0 and 1 that represents the accessibility via the internet of a vulnerability, such as 0.1 for low, 0.5 for medium, and 0.9 for high.

1) Using a tool or a service like CVE Prioritizer, an open-source tool that leverages the correlation between CVSS and Exploit Prediction Scoring System scores to improve efforts in fixing vulnerabilities.
2) The NIST Cybersecurity Framework can provide guidance and best practices for identifying, protecting, detecting, responding, and recovering from cyber incidents, and includes vulnerability management as a key function.

6.4.2. Using sentiment analysis

For enhancing the cybersecurity defense, sentiment analysis is also used in prioritizing vulnerability patching mechanisms that can provide additional insights and perspectives into the urgency, severity, and impact of the vulnerabilities and threat intelligence. We can apply sentiment analysis in the following use case scenarios:

1) To analyze the sentiment or tone of the news articles, blogs, forums, or social media that report or discuss the vulnerabilities.
2) To assign them a score or a level, such as positive, negative, or neutral, based on the emotions, opinions, or attitudes expressed in the text or speech.
3) To rank and schedule the patches or updates for the vulnerabilities, based on the combination of their sentiment score.
4) To monitor and track the changes in the sentiment or tone of the sources that report or discuss the vulnerabilities, and
5) To update or refine the ranking or schedule of the patches or updates based on the changes in the sentiment score or level.

6.5. Optimizing identity and access management

Optimizing identity and access management can enhance your security, compliance, and productivity, by mitigating the chances of data breaches, unauthorized entry, and non-compliance issues, and by improving the efficiency and scalability of the identity and access management process. Table 6 shows a detailed use case scenario for optimizing identity and case management.

Table 6. The use case scenarios for optimizing identity and access management

S. No.	Use cases
1	Establish clear goals and objectives for your identity and access management initiatives, and align them with your overall business strategies and priorities.
2	Conduct a risk assessment to identify and evaluate the current and potential threats and vulnerabilities in your identity and access management process, and to prioritize the actions and measures to mitigate them.
3	Regularly review and update the permissions and roles of your users, based on their job roles and responsibilities, and apply the principle of least privilege, which grants users the minimum level of access required to perform their tasks.
4	Enable single sign-on for the users, which allows them to access multiple applications and systems with one set of credentials and reduces the complexity and cost of managing passwords and accounts.
5	Implement multifactor authentication for your users, mandating the provision of two or more forms of evidence to authenticate their identity, like a password, a code, or a biometric.
6	Implement role-based access control for your resources, wherein permissions and access rights are allocated to users according to their roles rather than their specific identities.
7	Lower the exposure of your privileged accounts, which are accounts that have elevated or unrestricted access to your critical or sensitive resources, and implement strict controls and monitoring for them, such as password rotation, session recording, or audit logging.

Action 1	**Risk-based authentication**
Objective	To enhance the security and user experience of the authentication process.
Applications	by reducing the false positives or negatives, alert fatigue or overload, and unnecessary friction
Factors & methods	Using device, location, network, sensitivity, data integration, correlation, visualization, machine learning, artificial intelligence, or rule-based logic, to collect, aggregate, enrich, present, validate, and prioritize the security events or alerts that indicate a potential or actual cyber incident.
Action 2	**Continuous authentication**
Objective	To enhance the security and user experience of the authentication process
Applications	By detecting and preventing unauthorized access or misuse, and by eliminating the need for repeated or periodic authentication
Factors & methods	Through biometrics, keystroke dynamics, mouse movements, device orientation, location tracking, behavioral analytics, machine learning, artificial intelligence, or risk scoring, to capture, measure, and analyze the user behavior and activity
Action 3	**Automating user onboarding & offboarding**
Objective	To increase the efficiency and scalability of the user lifecycle management,
Applications	It improves consistency and compliance and increases productivity and satisfaction By reducing manual errors or delays.
Factors & methods	It can streamline and enhance user lifecycle management by creating, updating, or deleting user accounts and granting or revoking user access rights or permissions.
Action 4	**Self-service password reset**
Objective	To allow users to reset their passwords without the need to contact IT support or an administrator
Applications	By using an alternative method of identity verification, like email, phone, or security questions.
Factors & methods	Using various tools and techniques, such as password policy, password reset portal, password reset link, password reset code, password reset questions, or multifactor authentication

The following actions can be taken to achieve the proper identity and access management:

7. Conclusion

The healthcare sector is highly influenced by the latest technology including generative AI. With the cybersecurity concerns, the IT infrastructure of healthcare facilities is also upgrading. Integrating AI with a security approach is a key solution for healthcare facilities, but it requires careful implementation, testing, and oversight to get effective results. The validation of AI models and periodic training is compulsory for identifying emerging attack patterns while minimizing false positives. Apart from this, GenAI technologies have the potential to accelerate threat detection, enhance visibility across hybrid healthcare networks, improve third-party risk management, and empower proactive cybersecurity defenses. Although the healthcare sector is a frequent target for cybercriminals, the adoption of AI-powered security solutions has become necessary. As sophisticated and multifaceted cyber threats continue to escalate, generative AI's capabilities in threat detection, prediction, automation, and training will play a pivotal role in strengthening digital defenses. The study suggests that the proposed strategies have the potential to ensure proactive threat mitigation and provide robust security standards for real-time anomaly detection. Moreover, by implementing the five proposed methods, healthcare facilities can effectively safeguard sensitive patient data and secure their physical and digital infrastructures against evolving threats.

Ethical Statement

This study does not contain any studies with human or animal subjects performed by any of the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Author Contribution Statement

Shahazad Niwazi Qurashi: Conceptualization, Methodology, Investigation, Data curation, Writing – original draft, Supervision, Project administration. **Farrukh Sobia:** Conceptualization, Data curation, Writing – original draft. **Wafa A. Hetany:** Writing – review & editing. **Hani Sultan:** Visualization.

Supplementary Information

The supplementary file is available at https://doi.org/10.47852/bonviewMEDIN52024121.

References

[1] Lin, H. (2024). Artificial intelligence with great potential in medical informatics: A brief review. *Medinformatics*, *1*(1), 2–9. https://doi.org/10.47852/bonviewMEDIN42022204

[2] Vukotich, G. (2023). Healthcare and cybersecurity: Taking a Zero Trust approach. *Health Services Insights*, *16*, 11786329231187826. https://doi.org/10.1177/11786329231187826

[3] Yinka-Banjo, C., & Ugot, O. A. (2020). A review of generative adversarial networks and its application in cybersecurity. *Artificial Intelligence Review*, *53*, 1721–1736. https://doi.org/10.1007/s10462-019-09717-4

[4] Inkster, B., Knibbs, C., & Bada, M. (2023). Cybersecurity: A critical priority for digital mental health. *Frontiers in Digital Health*, *5*, 1242264. https://doi.org/10.3389/fdgth.2023.1242264

[5] Yeng, P. K., Nweke, L. O., Yang, B., Ali Fauzi, M., & Snekkenes, E. A. (2021). Artificial intelligence–based framework for analyzing health care staff security practice:

Mapping review and simulation study. *JMIR Medical Informatics*, *9*(12), e19250. https://doi.org/10.2196/19250

[6] Arshad, S., Arshad, J., Khan, M. M., & Parkinson, S. (2021). Analysis of security and privacy challenges for DNA-genomics applications and databases. *Journal of Biomedical Informatics*, *119*, 103815. https://doi.org/10.1016/j.jbi.2021.103815

[7] Roosan, D., Wu, Y., Tatla, V., Li, Y., Kugler, A., Chok, J., & Roosan, M. R. (2022). Framework to enable pharmacist access to health care data using Blockchain technology and artificial intelligence. *Journal of the American Pharmacists Association*, *62*(4), 1124–1132. https://doi.org/10.1016/j.japh.2022.02.018

[8] Almaiah, M. A., Ali, A., Hajjej, F., Pasha, M. F., & Alohali, M. A. (2022). A lightweight hybrid deep learning privacy preserving model for FC-based industrial internet of medical things. *Sensors*, *22*(6), 2112. https://doi.org/10.3390/s22062112

[9] Nayak, J., Meher, S. K., Souri, A., Naik, B., & Vimal, S. (2022). Extreme learning machine and Bayesian optimization-driven intelligent framework for IoMT cyber-attack detection. *The Journal of Supercomputing*, *78*(13), 14866–14891. https://doi.org/10.1007/s11227-022-04453-z

[10] Salim, M. M., & Park, J. H. (2022). Federated learning-based secure electronic health record sharing scheme in medical informatics. *IEEE Journal of Biomedical and Health Informatics*, *27*(2), 617–624. https://doi.org/10.1109/JBHI.2022.3174823

[11] Ramasamy, L. K., Khan, F., Shah, M., Prasad, B. V. V. S., Iwendi, C., & Biamba, C. (2022). Secure smart wearable computing through artificial intelligence-enabled internet of things and cyber-physical systems for health monitoring. *Sensors*, *22*(3), 1076. https://doi.org/10.3390/s22031076

[12] Wahab, F., Zhao, Y., Javeed, D., Al-Adhaileh, M. H., Almaaytah, S. A., Khan, W., . . . , & Kumar Shah, R. (2022). [Retracted] an AI-driven hybrid framework for intrusion detection in IoT-enabled E-Health. *Computational Intelligence and Neuroscience*, *2022*(1), 6096289. https://doi.org/10.1155/2022/6096289

[13] Ali, M., Naeem, F., Tariq, M., & Kaddoum, G. (2022). Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey. *IEEE Journal of Biomedical and Health Informatics*, *27*(2), 778–789. https://doi.org/10.1109/JBHI.2022.3181823

[14] Radanliev, P., De Roure, D., Maple, C., & Ani, U. (2022). Super-forecasting the 'technological singularity' risks from artificial intelligence. *Evolving Systems*, *13*(5), 747–757. https://doi.org/10.1007/s12530-022-09431-7

[15] Biasin, E., & Kamenjašević, E. (2022). Cybersecurity of medical devices: New challenges arising from the AI Act and NIS 2 Directive proposals. *International Cybersecurity Law Review*, *3*(1), 163–180. https://doi.org/10.1365/s43439-022-00054-x

[16] Horowitz, M. C., Kahn, L., Macdonald, J., & Schneider, J. (2024). Adopting AI: How familiarity breeds both trust and contempt. *AI & Society*, *39*(4), 1721–1735. https://doi.org/10.1007/s00146-023-01666-5

[17] Kelly, B., Quinn, C., Lawlor, A., Killeen, R., & Burrell, J. (2023). Cybersecurity in Healthcare. In H. Sakly, K. Yeom, S. Halabi, M. Said, J. Seekins & M. Tagina (Eds.), *Trends of artificial intelligence and big data for E-Health* (pp. 213–231). Switzerland: Springer. https://doi.org/10.1007/978-3-031-11199-0_11

[18] Oniani, D., Hilsman, J., Peng, Y., Poropatich, R. K., Pamplin, J. C., Legault, G. L., & Wang, Y. (2023). Adopting and expanding ethical principles for generative artificial intelligence from military to healthcare. *NPJ Digital Medicine*, *6*(1), 225. https://doi.org/10.1038/s41746-023-00965-x

[19] Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., . . . , & Sarwat, A. I. (2023). Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. *Sensors*, *23*(8), 4060. https://doi.org/10.3390/s23084060

[20] Barbaria, S., Mahjoubi, H., & Rahmouni, H. B. (2023). A novel blockchain-based architectural modal for healthcare data integrity: Covid19 screening laboratory use-case. *Procedia Computer Science*, *219*, 1436–1443. https://doi.org/10.1016/j.procs.2023.01.433

[21] Selvarajan, S., & Mouratidis, H. (2023). A quantum trust and consultative transaction-based blockchain cybersecurity model for healthcare systems. *Scientific Reports*, *13*(1), 7107. https://doi.org/10.1038/s41598-023-34354-x

[22] Cartwright, A. J. (2023). The elephant in the room: Cybersecurity in healthcare. *Journal of Clinical Monitoring and Computing*, *37*(5), 1123–1132. https://doi.org/10.1007/s10877-023-01013-5

[23] Silvestri, S., Islam, S., Papastergiou, S., Tzagkarakis, C., & Ciampi, M. (2023). A machine learning approach for the NLP-based analysis of cyber threats and vulnerabilities of the healthcare ecosystem. *Sensors*, *23*(2), 651. https://doi.org/10.3390/s23020651

[24] Rubinic, I., Kurtov, M., Rubinic, I., Likic, R., Dargan, P. I., & Wood, D. M. (2024). Artificial intelligence in clinical pharmacology: A case study and scoping review of large language models and bioweapon potential. *British Journal of Clinical Pharmacology*, *90*(3), 620–628. https://doi.org/10.1111/bcp.1589

[25] Messinis, S., Temenos, N., Protonotarios, N. E., Rallis, I., Kalogeras, D., & Doulamis, N. (2024). Enhancing Internet of Medical Things security with artificial intelligence: A comprehensive review. *Computers in Biology and Medicine*, *170*, 108036. https://doi.org/10.1016/j.compbiomed.2024.108036

[26] Zhan, Y., Ahmad, S. F., Irshad, M., Al-Razgan, M., Awwad, E. M., Ali, Y. A., & Ayassrah, A. Y. B. A. (2024). Investigating the role of Cybersecurity's perceived threats in the adoption of health information systems. *Heliyon*, *10*(1), e22947. https://doi.org/10.1016/j.heliyon.2023.e22947

[27] Shaikh, T. A., Rasool, T., & Verma, P. (2023). Machine intelligence and medical cyber-physical system architectures for smart healthcare: Taxonomy, challenges, opportunities, and possible solutions. *Artificial Intelligence in Medicine*, *146*, 102692. https://doi.org/10.1016/j.artmed.2023.102692

[28] Mylrea, M., & Robinson, N. (2023). Artificial Intelligence (AI) trust framework and maturity model: Applying an entropy lens to improve security, privacy, and ethical AI. *Entropy*, *25*(10), 1429. https://doi.org/10.3390/e25101429

How to Cite: Qurashi, S. N., Sobia, F., Hetany, W. A., & Sultan, H. (2025). Enhancing Cybersecurity Defenses in Healthcare Using AI: A Pivotal Role in Fortifying Digital Health Infrastructure. *Medinformatics*. https://doi.org/10.47852/bonviewMEDIN52024121

Abbreviations

GAN	Generative adversarial network
ML	Machine learning
AI	Artificial intelligence
IoT	Internet of Things
EMR	Electronic medical record
HIPAA	Health Insurance Portability and Accountability Act
NLP	Natural language processing
EHR	Electronic health record
DNA	Deoxyribonucleic acid
IIoT	Industrial Internet of Things
ToN-IoT	Telemetry and network Internet of Things
CNN	Convolutional neural network
IoT-CPS	Internet of Things – Cyber-physical systems
GRU	Gated recurrent unit
CIC DDoS	Canadian Institute for Cybersecurity Distributed Denial of Service
DNN	Deep neural network
CuBLSTM	Cuda-bidirectional long short-term memory
FL	Federated learning
PHI	Protected health information
ICU	Intensive care unit
ICT	Information and communications technology
BERT	Bidirectional encoder representations from transformers
XGBoost	eXtreme Gradient Boosting
LLM	Large language models
MCPS	Medical cyber-physical systems
SMS	Short Message Service
IP	Internet Protocol
CVSS	Common Vulnerability Scoring System
EPSS	Exploit Prediction Scoring System Scores
NIST	National Institute of Standards and Technology