American Journal of Medical Science and Innovation (AJMSI)

ISSN: 2836-8509 (ONLINE)

VOLUME 4 ISSUE 2 (2025)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Medical Science and Innovation (AJMSI)

Volume 4 Issue 2, Year 2025
ISSN: 2836-8509 (Online)
DOI: https://doi.org/10.54536/ajmsi.v4i2.6178
https://journals.e-palli.com/home/index.php/ajmsi

Artificial Intelligence for Strengthening Cybersecurity in U.S. Healthcare Systems

Barbara Aryeley Aryee[1], Jehoiarib Umoren[2*], Kwadwo Adu Agymang[1]

Article Information

Received: September 20, 2025
Accepted: October 23, 2025
Published: December 30, 2025

Keywords

Artificial Intelligence, Cybersecurity, Data Protection, Healthcare, Threat Detection, U.S. Systems

ABSTRACT

The US healthcare industry is grappling with a new level of cybersecurity threats. In fact, data breaches reached 275 million people just in 2024, which is equal to 82% of the U.S. population. All the old ways of doing cybersecurity remain insufficient in the face of ever-evolving threats. These traditional methods involve signature and perimeter-based detection techniques, as well as rule-based access policies. Even with robust cybersecurity investment, 92% of healthcare providers were hit by data breaches in the past few years. This paper explores the use of artificial intelligence technologies to improve cybersecurity in US healthcare systems. This study uses a systematic literature review approach. The research examines today's threat landscapes, traditional security shortcomings and AI-driven approaches. The study synthesizes data from various sources, including recent studies published in the academic literature, online databases and industry reports covering 2019-2025. The results showed that AI-based methods outperform the traditional techniques. These methods include machine learning based anomaly detection, deep learning models for zero-day exploit detection, and natural language processing (NLP)-based threat analysis. However, implementation challenges persist. These difficulties are the adversarial attacks on AI systems, the transparency of the algorithm, false positives, and HIPAA compliance. The study concludes that artificial intelligence offers transformative potential for healthcare cybersecurity; thus, successful deployment requires careful integration with existing infrastructure, continuous model updating, and collaboration between AI systems and human security specialists.

INTRODUCTION

The modern healthcare situation in the United States is facing an unprecedented integration of technological improvements with a lack of security (Wang *et al.,* 2021). According to Zhang & Saltman (2022), the healthcare organizations have implemented electronic health records, telemedicine platforms and interconnected medical devices quickly to improve the care and efficiency of their operations towards taking care of their patients (Sani & Aryee, 2025). However, it is this digital transformation that simultaneously increases the size of the attack surface that malicious actors can use. As a result, the healthcare industry has become one of the most hit sectors by cyberattacks, with breaches affecting millions of patient records every year and putting the integrity of the data and the safety of patients at risk.

The specific characteristics of healthcare systems aggravate these cybersecurity problems. The healthcare institutions have to balance high security requirements with the need to access data instantly to make clinical decisions, unlike other industries (Li *et al.,* 2025). To provide clinicians with unimpeded access to patient data during emergencies, clinicians demand penetration into the system, which is an aspect that opens possible entry points for cyber threats (Li *et al.,* 2025). Additionally, the healthcare ecosystem is an intricate network of hospitals, clinics, insurance services, pharmaceutical firms and medical device production, every one of which is a potential vulnerability in the overall security design (Yaqoob *et al.* 2019).

Conventional cybersecurity methods have been unable to keep up with the evolving cloud of threats that health systems face (Salama *et al.,* 2024). Per Soe *et al.* (2019), standard rule-based security mechanisms depend on previously known signatures and attack techniques and thus cannot handle new threats and determined attackers. The increasing volume and velocity of data transmitted through care delivery networks have surpassed human analytic ability, which introduces blind spots into security monitoring. These failures have led to disastrous breaches, including ransomware attacks that have disabled hospital functioning and threatened care delivery to patients.

AI provides a non-negligible potential evolution of the fight against these cybersecurity challenges in health (Laith *et al.,* 2025). Machine learning models can process large amounts of network data and help detect abnormal patterns, which may indicate suspicious activity indicative of security threats (Narteh-Kofi *et al.,* 2025; Gokah *et al.,* 2025). Applying deep learning models to zero-day exploits and unreported attack vectors. With the help of natural language processing, this facilitates automatic examination of security logs and threat intelligence documents (Ibraheem & Tosho, 2024). Such approaches can leverage AI to respond to emerging threats, learn

[1] Department of Information Systems, East Tennessee State University (ETSU), Johnson City, TN, USA
[2] Department of Supply Chain Management, University of Houston, C.T. Bauer College of Business, Houston, Texas, USA
* Corresponding author's e-mail: barbaraaryee@gmail.com

from new patterns of attack and offer predictive abilities that foresee security incidents before they occur.

Conceptually, the integration of artificial intelligence into the cybersecurity mechanisms of healthcare organizations provides both opportunities and threats. On the one hand, AI-powered processes can greatly enhance the accuracy of threat identification, speed up the incident remedial operation and facilitate the process of resource distribution in limited security resources (Narteh-Kofi *et al.,* 2025). On the other hand, the implementation of AI systems in healthcare security requires strict examination in terms of algorithm transparency, false positives and susceptibility of AI systems to advanced adversarial attacks. The institutions that act in the healthcare industry need to skillfully strike a balance between the demands of the regulatory regulations, the most important of which is HIPAA and the realities of implementing AI-bound security measures.

This research explores the application of artificial intelligence technologies in a bid to strengthen cybersecurity in the healthcare systems of the United States. The paper analyzes the current threat environment, the existing security paradigms, AI-based methodologies applicable to healthcare cybersecurity, and the implementation challenges associated with them. The objective of this paper is to develop a framework that explains how artificial intelligence can be used to improve the cybersecurity position of health facilities and maintain the accessibility and reliability that cannot be compromised under any circumstances in managing patients. Through a failover method approach, an in-depth examination of technological strengths and opportunities, deployment initiatives and organizational factors, this article aims to add to the growing body of research at the intersection of artificial intelligence, cybersecurity and health informatics.

LITERATURE REVIEW

In modern practice, the increasingly growing number of cyber adversities targeted at medical facilities reminds us of the necessity of advanced defense systems that can protect confidential patient information and medical facilities. The growing complexity of these threats requires that it be echoed in a paradigm change whereby adaptive architectures are needed to be capable of predictively countering the attempts of intrusion with greater accuracy than ever before. This review is a synthesis of the literature on the case of applications of artificial intelligence in healthcare cybersecurity and how conventional security models have developed into intelligent and adaptive defense models. It sheds light on the future and performance of AI-based interventions in enhancing the digital health ecosystem by critically assessing the work of pioneers and novel approaches and innovations.

Cybersecurity Threat Landscape in Healthcare Systems

This section examines the current state of cybersecurity threats targeting healthcare organizations.

Abirami and Parameshwari (2025) assessed the changing cybersecurity threat environment that now surrounds smart and interconnected healthcare systems, which highlights the dualism in technological progress in the clinical environment. The authors also carefully reported the way the implementation of new technologies by health-care organizations, with the clear intention of improving the treatment of patients and the efficiency of the work process, has both created new attack vectors and new vulnerabilities. Their research pointed out the growing influence of cybercriminals to target healthcare-sector information using network access to install ransomware to effectively paralyse vital services or encrypt important files until they can collect ransom payments. The researchers observed that healthcare organizations are highly prone to falling under ransom demands due to the time-sensitive nature of medical services, where any downturn in the availability of data may directly affect patients and their care in a direct and potentially life-threatening manner. Their study also found the vulnerability to network-based medical devices, where failure or hacking may lead to inaccuracy in dispensing medicine or device involvement.

A study conducted by Kioskli *et al.* (2021) involved a systematic evaluation of the vulnerabilities and issues of cybersecurity that disproportionately impact the critical information infrastructure of the healthcare industry. Their research found that the healthcare sector is underprepared and somewhat ill-equipped to deal with advanced cyberattacks, with bad actors taking advantage of dormant flaws to exploit them more than ever. The authors have reported that the spread of medical equipment and intelligent devices, coupled with the intricacy of their operations and the existence of incompatible systems, exposes healthcare organizations to a range of malware, especially ransomware. Their discussion shows that such security breaches foster undermined access to care, low-quality care, lack of safety and poor patient care delivery. Their research in a critical analysis of current standards of healthcare security reveals inconsistencies and a lack of implementation guidelines that make protective measures ineffective and challenging to implement. In turn, the researchers propose the introduction of living labs as a new framework to apply the valid practice of implementing cybersecurity effectively and provide suggestions on creating a solid base that would contribute to gaining more knowledge about the intricate nature of cybersecurity issues in the healthcare industry.

Similarly, Burrell (2024) analysed the complexity in managing cybersecurity risk in the healthcare field, especially in the context of the scale of potential damage to the stability of the economy through terrorist attacks, epidemic outbreaks and natural disasters. The analysis has emphasized problems created by the privatization of healthcare assets and has noted that greater collaboration and information sharing between the public and the private sectors is urgently required. In addition, Burrell

(2024) documents how the COVID-19 outbreak triggered the digitalization of the medical sector and thus increased the risks of cyber threats and the attack surface. His research gave grim estimates of the economic cost of cybercrime, with projections reaching over ten trillion United States dollars in 2023, and with the amount expected to skyrocket to almost twenty-four trillion United States dollars within the following four years. His analysis has revealed human error as the most common cause of cybersecurity attacks, as they were found to be ninety-five percent of reported cases and insider threats were found to be a significant factor that predisposes organisations to vulnerabilities.

Frumento (2019) examined historical and present challenges for healthcare cybersecurity in response to the digitalisation of healthcare, including healthcare's early use of information and communication technologies. His research canvassed how healthcare has transformed from its early days of computerizing hospitals to being one of the most attacked and lucrative domains for cyberattacks and cyberterror abuses. According to Frumento's research, valuable data glut, healthcare as critical infrastructure and the prevalence of mobile health created a perfect storm for cybercriminals. His study detailed the enormous digital overhaul in which both healthcare providers and users (patients) engage; it will transform not only service delivery, but how services are consumed. His investigation contributed to a proposal of Hospital 2.0 and patient ecosystems, looking at how the new workflow paradigms were changing in healthcare application scenarios. In addition, his study offered a detailed investigation of current and future threat environments, which were annotated with analysis such as cyberterrorism, cybercrime targeting approaches and emerging threats for mobile health (mHealth) systems, providing an essential perspective for apprehending healthcare cybersecurity issues from numerous angles.

The bar chart above shows the healthcare data breaches

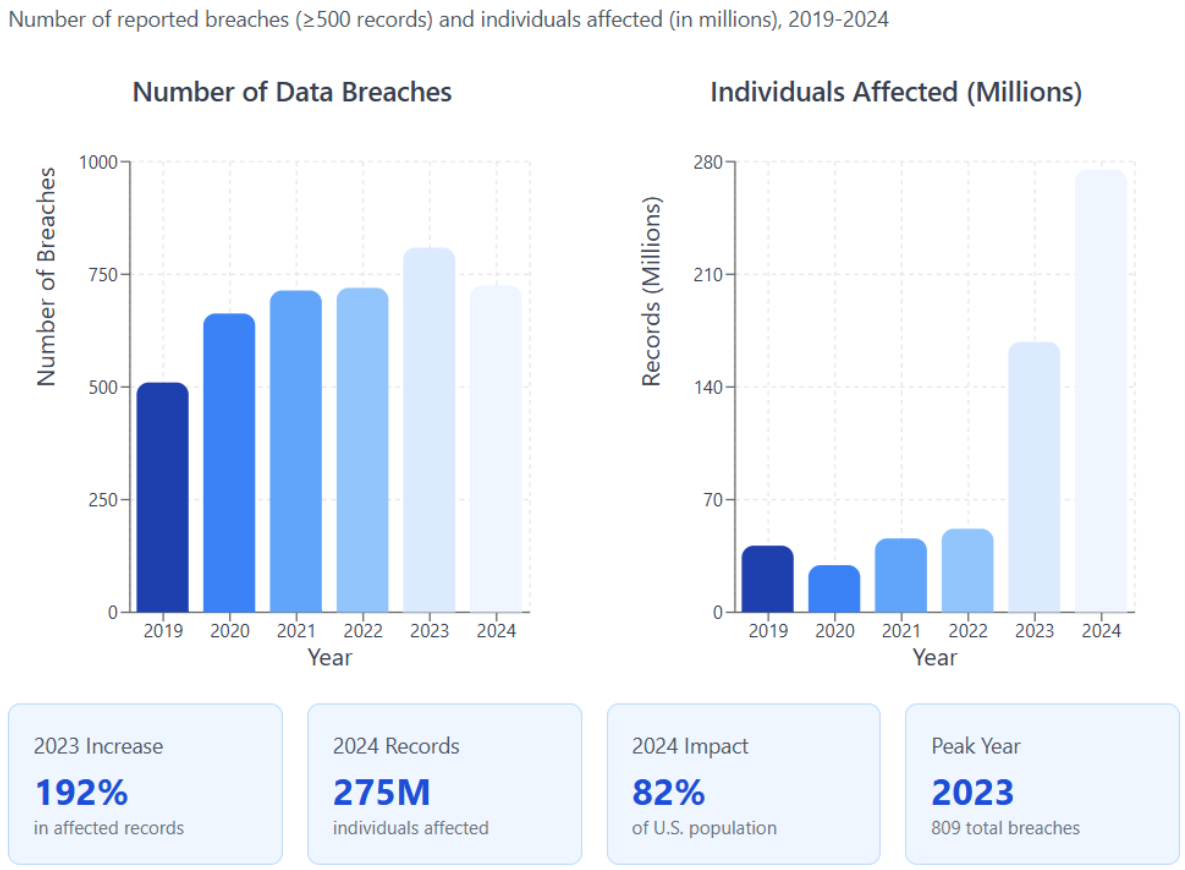

Figure 1: U.S. Healthcare Data Breaches: Rising Threat Landscape
Data Sources: U.S. Department of Health and Human Services Office for Civil Rights (HHS OCR); HIPAA Journal Healthcare Data Breach Reports (2019-2024). Data represents breaches affecting 500 or more records as reported to HHS OCR under the HIPAA Breach Notification Rule.

of 500 or more records (reported to HHS) that occurred from 2019 through 2024 as reported by the U.S. Department of Health and Human Services Office for Civil Rights website. The graph shows steady growth in breach incidents and reaches a peak with 809 reported breaches in 2023. The volume of individuals whose data is impacted by those breach incidents only gets worse, with a significant trend across the years; 168 million

records were breached in 2023 and 275 million in 2024. This also means that this stunning increase in 2024 is the equivalent of a staggering 82% of all Americans being victims of breached healthcare records. These numbers validate what security experts have been warning: the cybersecurity threat landscape against health care companies is intensifying and stronger defensive measures are a must.

Traditional Cybersecurity Approaches and Their Limitations in Healthcare

This part reviews the traditional cybersecurity models and technologies that are being implemented in health contexts. Empirical studies that evaluate the effectiveness of traditional security solutions, including firewalls, intrusion detection systems, antivirus programs and rule-based access controls, in the context of healthcare delivery specifically are evaluated in this literature review.

The conventional cybersecurity approaches implemented in the healthcare industry have, for a long period, been based on models of protection on the perimeter, signature-based detection systems and rule-based access control. These strategies became reality in a time when medical information technology ecosystems were somewhat primitive and not as interrelated as current ones (Hermes *et al.* 2020). The theoretical basis behind traditional frameworks was that the defense of external boundaries would be adequate in the protection of internal networks and data repositories against the intrusion of adversaries (Khraisat & Alazab, 2021; Adukpo & Bethel, 2025). In line with this, healthcare organizations have adopted firewalls, anti-malware suites, as well as intrusion detection systems as underlying defense mechanisms aimed at preventing unauthorized ingress. With the combination of the rising digital transformation in the field, due to the parallel growth of networked medical equipment and clouded health information infrastructures, these outdated defense stances have proven to harbor material gaps. The complex interdependencies and increased attack surface that have since become standard to the modern healthcare ecosystems make the perimeter-based models all the more ineffective.

The failure of signature-based detector solutions is a structural constraint of traditional cybersecurity measures in the healthcare sector. Olatuyi (2025) recorded that traditional intrusion detection systems are based on the existing attack patterns and known threat signatures that make them ineffective in preventing new exploits and zero-day vulnerabilities. The systems work on the principle of matching network traffic and system actions to curated databases of known malicious signatures, and therefore assume a reactive posture in nature, which fails when faced with unexplored attack vectors. Khan and Herrmann (2019) highlighted that the unlimited expansion of network traffic and user data has exceeded the processing capacity of the traditional intrusion detection systems, especially in the healthcare setting, where the amount and pace of data transfer surpass the analytical limits of the rule-based systems. The very size of the continuous data streams, therefore, elicits the responsiveness and scaling capabilities of the old-fashioned detection frameworks. In addition, the large number of false positives created by traditional detection systems creates alert fatigue in security staff, making the overall threat-response performance worse and the probability of real security events being ignored through the noise of false alarms higher.

Vulnerabilities of the legacy systems are still unresolved weakness in traditional healthcare cybersecurity. As shown in a recent study by Olatuyi (2025), it was revealed that about eighty-five percent of medical institutions continue to use outdated systems or infrastructure, with many facilities relying on the unsupported operating systems, including Windows XP and legacy firmware, to which vendors no longer provide security patches. These outdated platforms are unable to connect with the latest security solutions and lack the functions of supporting the latest encryption standards or authentication measures. Naghib *et al.* (2023) also reported that medical devices are frequently poorly secured in terms of their security, have low-quality design features and lack a thorough authentication system, which makes them especially susceptible to use by attackers. Conceptually, this challenge is further exacerbated because healthcare organisations are faced with heavy operational burdens that hinder the ability to promptly replace or upgrade outdated equipment; these devices need to be available twenty-four hours a day to continue to provide patient care, thus they cannot be as easily put offline to be repaired or patched to prevent security breaches.

The tension between clinical operational requirements and security requirements is a long-standing problem that conventional cybersecurity methods cannot effectively address. Traditional access control systems focus on authentication strictness and authorization controls, which provide inflexible protocols that must undergo several checks before giving users access to the system (Kizza 2024). Nevertheless, medical conditions require patients to be attended to as quickly and without distraction as possible and a few seconds can be devastating in a medical crisis. According to Alsubaei *et al.* (2024), the conventional approaches to security usually suppress fast access to information, which may adversely affect patient care in an emergency, when clinicians need quick access to medical records, laboratory findings and other imaging data. In addition, the non-uniform nature of healthcare information technology ecosystems, which most commonly involve legacy systems, new cloud-based applications or proprietary medical device interfaces using different security standards, presents interoperability challenges that conventional security models have difficulty providing. The need to facilitate smooth data transfer across the various systems comes against network segmentation approaches taken by conventional security paradigms to restrict the potential breaches, hence compelling healthcare organizations to

decide on operational effectiveness versus the strength of the security in a manner that other sectors do not experience consistently.

Artificial Intelligence Techniques and Methodologies for Cybersecurity

This aspect surveys artificial intelligence technologies applicable to cybersecurity challenges. The literature review examines research on machine learning algorithms for threat detection, including supervised, unsupervised and reinforcement learning approaches.

The rise of artificial intelligence (AI) has become a game-changer in combating the emerging patterns of cybersecurity threats to healthcare systems (Neoaz, 2025; Narteh-Kofi *et al.,* 2025). ML algorithms inspect large-scale network traffic data to detect abnormal patterns that may reveal cyberattacks or security breaches (Apruzzese *et al.,* 2023). With reference to malware, phishing and intrusion detection, deep learning methods, including CNNs (convolutional neural networks) and RNNs (recurrent neural networks), outperform traditional signature-based approaches (Alshoulie & Mehmood, 2025). For example, natural language processing can provide automated means for analyzing security logs, threat intelligence reports and vulnerability disclosures to detect threats in real-time and prioritize defensive responses (Kasri *et al.,* 2025). Some researchers have leveraged reinforcement learning methods to construct adaptive security policies that can dynamically adapt themselves according to the dynamics of threat environments and allocate resources for defense techniques optimally (Han *et al.,* 2021; Umoren *et al.,* 2025).

Application of supervised learning methods to cybersecurity requires the presence of annotated datasets that specify the network traffic, system behavior, as well as file characteristics as benign or malicious. Support vector machines (SVMs) have become a feature of intrusion detection systems, due to their ability to operate in high-dimensional feature space and provide strong generalization (Ahmad *et al.,* 2021). Random Forests and Gradient Boosting, which are types of ensemble techniques that combine many decision trees, are more cost-effective at providing predictive fidelity and reducing false-positive rates in threat detection (Khraisat *et al.,* 2019). Multi-layer neural networks enable automatic salient features to be extracted from raw data, bypassing the time-consuming feature engineering (which is traditionally a lab-intensive process) process that previously required substantial domain knowledge (Chinnasamy *et al.,* 2015). However, the monitored approaches to learning face significant challenges in the field of cybersecurity. The continuous change in the vectors of attacks, the lack of labeled malicious data and the high level of imbalance of classes when the illicit activity occupies an insignificant percentage of the total traffic make the effectiveness of these models questionable (Azam *et al.* 2023; Umoren *et al.,* 2025).

In recent literature, the unsupervised learning schemes have become an interesting alternative to their more supervised counterparts, largely due to their ability to uncover abnormal patterns without the help of pre-labeled data. The clustering algorithms are used to group similar network behaviors or system events, including k-means, DBSCAN and hierarchical clustering, to isolate outliers that can indicate security threats (Nisioti et al, 2018). Autoencoders are neural networks that are trained to recreate their input and offer a strong method of identifying anomalies by indicating cases where the reconstruction error exceeds predetermined thresholds (Rezaiezadeh Roukerd *et al.,* 2024). Generative adversarial networks were also used to generate samples of attacks, thus boosting sparse training datasets and making detection models more resistant (Halvorsen *et al.,* 2024). Self-organising maps add a graphical layer that aids security analysts in understanding the layout of the network traffic as well as the identification of suspicious trends (Jayabharathi & Ilango, 2022). However, these benefits are accompanied by the fact that the unsupervised techniques often have high false-positive rates because not every anomaly detected is a factual threat; it is always difficult to distinguish between harmless and malicious anomalies (Abdallah & Otoom, 2022).

The implementation of artificial intelligence in cybersecurity systems should overcome several severe issues concerning adversarial attacks, model interpretability and computational efficiency (Zhang *et al.* 2022; Narteh-Kofi *et al.,* 2025). Research in adversarial machine learning has already shown that attackers can use inputs to make AI models provide incorrect predictions, which can potentially evade detection systems (Biggio and Roli, 2018). Explainable AI models like LIME, SHAP and attention mechanisms offer insight into the model decision-making logic, which is required to prove detections and comprehend the nature of attacks (Arrieta *et al.,* 2020). Threat detection in healthcare facilities in real-time requires AI models capable of handling streaming information at low latency and at high accuracy, which can be optimized by employing methods and streamlined designs (Arefin, 2024). Transfer learning methods allow models that are trained on data of a specific healthcare organization to be adapted to work in another organization with little extra training data, or deal with data scarcity and privacy issues (Iman *et al.,* 2023). The success of AI-based cybersecurity systems will not be limited to the level of algorithm sophistication, but also integration with the current security infrastructure, constant model updating to adapt to new threats, and interaction between AI systems and human security specialists who can offer subject-domain knowledge and contextual insights.

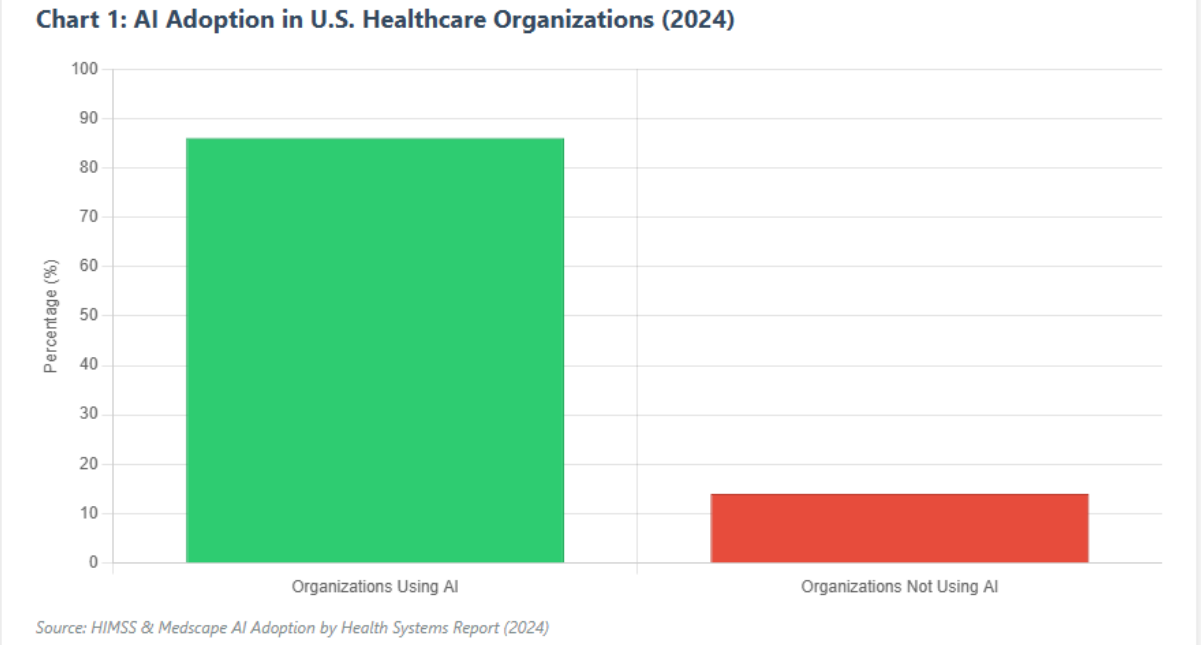

Figure 2: AI for Strengthening Cybersecurity in U.S. Healthcare Systems

The figure shows that 86% of US healthcare organizations have already started using AI, which informs a high degree of readiness for adopting AI-based cybersecurity tools (HIMSS & Medscape, 2024). Healthcare data breaches peaked at 809 incidents in 2023, with ransomware representing an average of 53.6% of all cyber incidents from 2014 to 2024, which emphasizes the need for machine learning algorithms that are not only able to detect Ransomware but also Data exfiltration attacks. Release of more than 180 million patient records in breach breaks record as a result of an increasingly sophisticated threat that traditional signature-based detection cannot sufficiently counter. Among healthcare organizations employing AI for cybersecurity, threat-hunting (32%) and anomaly detection (28%) are the top-use cases, which correspond to the notable supervised and unsupervised learning methods covered in current publications. Trending upwards, the prevalence of ransomware attack recovery times: more than one month increased from 28% in 2023 to 37% in 2024, further underlining the importance of real-time AI detection that can operate on streaming data with low latency and high accuracy.

Applications of AI in Healthcare Cybersecurity: Current State and Effectiveness

This section examines empirical studies and case analyses of AI implementations in healthcare security contexts. The literature review analyzes research documenting real-world deployments of AI-driven security systems in healthcare organizations, including their performance metrics, accuracy rates and operational outcomes.

Ozkan-Okay *et al.* (2023) present a survey that includes a critical assessment of the effectiveness of artificial intelligence and machine learning methods in the context of cybersecurity solutions. Their study methodically examines how machine learning, deep learning and reinforcement learning are applicable in the critical cybersecurity operations, such as malware detection, intrusion detection, vulnerability assessment and other critical areas. Their paper shows that machine-learning algorithms use statistical tools to identify patterns and anomalies in vast datasets, thus helping security analysts to identify previously unidentified threats with a higher degree of accuracy. The field of deep learning has had substantial promise in improving the precision and performance of cybersecurity systems, especially in image and speech recognition tasks, where it has demonstrated superiority to traditional methods. Besides, their study considers the use of ChatGPT-like AI tools regarding the area of cyber-related issues and evaluates both the beneficial and possibly harmful facets of this practice. The authors develop a set of research questions that help in offering a more comprehensive guideline for the study of AI and ML models' performance in the cybersecurity context. The challenges and limitations of these techniques are also discussed in the study, including the concerns of data quality, interpretability and vulnerability to adversarial attacks. On the whole, their study highlights the fact that the integration of machine learning, deep learning and reinforcement learning into the area of cybersecurity has tremendous potential in enhancing the performance of security-related mechanisms and improving security against cyberattacks.

A study by Zhang *et al.* (2023) provides an overall review of the existing literature on explainable artificial intelligence applying to cybersecurity. Their paper fills a significant knowledge gap in the area by targeting the capability of explainable AI to increase the level of transparency and interpretability in cyber defence systems. Their study justifies that, despite artificial intelligence-related methods

of identifying and preventing cyber attacks and threats being more efficient and advanced in comparison to the traditional signature-based and rule-based strategies of cybersecurity, most machine-learning-based and deep-learning-based methods are used in a black-box way. This implies that security specialists and the customers cannot describe how such processes could arrive at specific conclusions. The limitations of transparency and interpretability of current artificial intelligence methods reduce confidence of human users in the models applied to defence against cyber attacks, particularly in the current situation where cyber attacks are becoming more and more diverse and complex. Their paper highlights that the use of explainable AI in the development of cybersecurity models is a necessity to formulate more explainable models without compromising accuracy, nor permitting human users to understand, trust and control the next generation of cybersecurity mechanisms. Their study presents an in-depth and current overview of the explainable AI solutions that could be utilized to address the issues in the sphere of cybersecurity and thus addresses a major gap in the existing research.

Similarly, Algarni and Thayananthan (2025) analyze the nexus between cybersecurity and artificial intelligence-based assistive technologies in the digital health environment. Their study explicitly explores the effect of AI-based support systems on cybersecurity dynamics in digital healthcare solutions with a specific focus on the latent vulnerabilities that such technologies can bring about. The model suggested by the authors completes the AI-based assistive technology implementation with the implementation of emerging security technologies, the formation of full-scale risk management and a powerful evaluation framework. Their research methodically deals with the detection and management of cybersecurity threats posed by AI-based systems, particularly in the environment of digital healthcare applications. Their results indicated that the use of the AI-based risk and resilience assessment system can considerably improve the security status of the assistive technology systems, especially those supporting e-learning among the visually impaired individuals. Their quantitative data show that cybersecurity within the digital health environments becomes more resilient, especially in an area where the cybersecurity of the users of assistive technology in e-learning environments is mitigated. Generally, their study offers a comprehensive, academically sound method of enhancing AI-powered assistive technology within the digital health care context to achieve system resilience, decrease user-centered cybersecurity threats and increase the efficiency of professional e-learning experiences.

Research by Alzahrani (2023) suggests an artificial-intelligence-based convolutional neural network paradigm to detect cyber-attacks in the domain of medical and healthcare. Their research paper further sheds light on the rapidly growing field of healthcare cybersecurity, in which threats continue to spread and malicious organizations are still willing to go around regulatory controls and measures. Although the main reasons behind committing cyber-attacks have not seen significant changes over time, the opponents have perfected their tricks, thus making it hard to identify and contain the emerging threats using the traditional defensive tools. Therefore, the introduction of AI-based approaches provides an opportunity to enable cybersecurity experts to address the ever-changing threat of attackers. Their paper outlines an Ant-Colony-Optimization-based convolutional neural network architecture, which has been created in partnership with a specially-crafted dataset of web-attack examples to support the identification of cyber-attacks within the healthcare environment. The empirical evidence shows that the suggested framework is superior to modern methods, as it offers a more effective detection of cyber-incidents. Their results emphasize the massive use of cybersecurity systems in the healthcare sector to protect the well-being of patients, and the fact that solutions based on artificial intelligence significantly enhance such systems.

CONCLUSION

This paper evaluates the use of artificial intelligence to augment cybersecurity in US healthcare and identifies significant opportunities, as well as key challenges. The results indicated that healthcare is experiencing a growing cybersecurity crisis, with the 809 breaches that occurred in 2023, combined to expose more than 180 million patient records, which confirms an overwhelming threat environment where normal security tactics are insufficient. Traditional security approaches have limitations such as the inability to detect zero-day exploits, high false positive rates, a lack of mechanisms to scale with an expansion in data and conflicts between the requirements of security and clinical operations. Artificial Intelligence has transformative potential with its specific types, such as Machine Learning algorithms that can detect anomalies in the network traffic, Deep Learning models for advanced threat identification and Reinforcement Learning methods to learn adaptive security policies. The review reveals 86% of healthcare providers now use the advances in technology, including threat and anomaly detection. Nevertheless, there are still some important challenges that integration needs to confront, such as dealing with adversarial attacks, the requirement for model interpretability, computational efficiency for real-time detection and an XAI (explainable artificial intelligence) framework for transparency. Implementation success depends on the full integration into the existing foundation of constantly updated models, within a process and working practice that utilizes both artificial intelligence systems and human experts and also on institutional preparedness to sustain such operations based on artificial intelligence.

REFERENCES

Abdallah, E. E., & Otoom, A. F. (2022). Intrusion detection systems using supervised machine learning techniques: a survey. *Procedia Computer Science, 201*,

205-212.

Abirami, T., & Parameshwari, V. Cybersecurity Threat Landscape of Smart and Interconnected Healthcare Systems. In *Cybersecurity and Data Science Innovations for Sustainable Development of HEICC* (pp. 76-92). CRC Press.

Adukpo, T. K., & Bethel, J. O. (2025). Impact of macroeconomic factors on government spending in Ghana. *American Journal of Applied Statistics and Economics, 4*(1). https://doi.org/10.54536/ajase.v4i1.5833

Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies, 32*(1), e4150.

Algarni, A. M., & Thayananthan, V. (2025). Cybersecurity for Analyzing Artificial Intelligence (AI)-Based Assistive Technology and Systems in Digital Health. *Systems, 13*(6), 439.

Alshoulie, M., & Mehmood, A. (2025). Deep learning approaches for malware detection: A comprehensive review of techniques, challenges, and future directions. *IEEE Access*.

Alzahrani, A. A. (2023). *Using Artificial Intelligence and Cybersecurity in Medical and Healthcare Applications*. Alzahrani, AA.

Apruzzese, G., Laskov, P., Montes de Oca, E., Mallouli, W., Brdalo Rapa, L., Grammatopoulos, A. V., & Di Franco, F. (2023). The role of machine learning in cybersecurity. *Digital Threats: Research and Practice, 4*(1), 1-38.

Arefin, S. (2024). Strengthening healthcare data security with AI-powered threat detection. *International Journal of Scientific Research and Management (IJSRM), 12*(10), 1477-1483.

Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., ... & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information fusion, 58*, 82-115.

Azam, Z., Islam, M. M., & Huda, M. N. (2023). Comparative analysis of intrusion detection systems and machine learning-based model analysis through decision tree. *Ieee Access, 11*, 80348-80391.

Biggio, B., & Roli, F. (2018, October). Wild patterns: Ten years after the rise of adversarial machine learning. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 2154-2156).

Burrell, D. N. (2024). Understanding healthcare cybersecurity risk management complexity. *Land Forces Academy Review, 29*(1), 38-49.

Chinnasamy, R., Subramanian, M., Easwaramoorthy, S. V., & Cho, J. (2025). *Deep learning-driven methods for network-based intrusion detection systems: A systematic review.* ICT Express.

Frumento, E. (2019). Cybersecurity and the evolution of healthcare: challenges and threats behind its evolution. In *M_Health current and future applications* (pp. 35-69). Cham: Springer International Publishing.

Gokah, B. E., Amoako, E. K., Adom, S. G., Abakah, L. K., & Sampson, E. (2025). AI-driven user experience (UX) frameworks to enhance trust and security in U.S. online banking. *Finance & Accounting Research Journal, 7*(9), 465–478. https://doi.org/10.51594/farj.v7i9.2069

Halvorsen, J., Izurieta, C., Cai, H., & Gebremedhin, A. (2024). Applying generative machine learning to intrusion detection: A systematic mapping study and review. *ACM Computing Surveys, 56*(10), 1-33.

Han, D., Wang, Z., Zhong, Y., Chen, W., Yang, J., Lu, S., ... & Yin, X. (2021). Evaluating and improving adversarial robustness of machine learning-based network intrusion detectors. *IEEE Journal on Selected Areas in Communications, 39*(8), 2632-2647.

Hermes, S., Riasanow, T., Clemons, E. K., Böhm, M., & Krcmar, H. (2020). The digital transformation of the healthcare industry: exploring the rise of emerging platform ecosystems and their influence on the role of patients. *Business Research, 13*(3), 1033-1069.

Ibraheem, I. O., & Tosho, A. U. (2024). Zero-day attack vulnerabilities: mitigation using machine learning for performance evaluation. *Journal of Computers for Society, 5*(1), 43-58.

Iman, M., Arabnia, H. R., & Rasheed, K. (2023). A review of deep transfer learning and recent advancements. *Technologies, 11*(2), 40.

Jayabharathi, S., & Ilango, V. (2022, September). Anomaly detection using machine learning techniques: A systematic review. In *International Conference on Advances in Data-Driven Computing and Intelligent Systems* (pp. 553-572). Singapore: Springer Nature Singapore.

Kasri, W., Himeur, Y., Alkhazaleh, H. A., Tarapiah, S., Atalla, S., Mansoor, W., & Al-Ahmad, H. (2025). From vulnerability to defense: The role of large language models in enhancing cybersecurity. *Computation, 13*(2), 30.

Khan, Z. A., & Herrmann, P. (2019). Recent advancements in intrusion detection systems for the Internet of Things. *Security and Communication Networks, 2019*(1), 4301409.

Khraisat, A., & Alazab, A. (2021). A critical review of intrusion detection systems in the Internet of Things: techniques, deployment strategy, validation strategy, attacks, public datasets, and challenges. *Cybersecurity, 4*(1), 18.

Kioskli, K., Fotis, T., & Mouratidis, H. (2021, August). The landscape of cybersecurity vulnerabilities and challenges in healthcare: Security standards and paradigm shift recommendations. In *Proceedings of the 16th International Conference on Availability, Reliability and Security* (pp. 1-9).

Kizza, J. M. (2024). Access control and authorization. In *Guide to Computer Network Security* (pp. 195-214). Cham: Springer International Publishing.

Laith, A. E., Jaouni, H., & Mihyar, A. (2025). Addressing cyberbiosecurity challenges in the modern era of biotechnology and artificial intelligence: cyberbiosecurity in the age of biotechnology and AI. Global Biosecurity.

Li, S., Surineni, K., & Prabhakaran, N. (2025). Cyber-Attacks on Hospital Systems: A Narrative Review. The American *Journal of Geriatric Psychiatry: Open Science, Education, and Practice*.

Naghib, A., Jafari Navimipour, N., Hosseinzadeh, M., & Sharifi, A. (2023). A comprehensive and systematic literature review on the big data management techniques in the Internet of Things. *Wireless Networks, 29*(3), 1085-1144.

Narteh-Kofi, E., Asamoah, E., Adukpo, T. K., Mensah, N. (2025). Mergers and Acquisitions in the U.S. Capital Market: Theoretical Foundations, Market Dynamics and Strategic Implications. *EPRA International Journal of Economics, Business and Management Studies (EBMS), 12*(3), 71-80. https://doi.org/10.36713/epra20500

Narteh-Kofi, E., Raji, Y. M., Asamoah, E., & Adukpo, T. K. (2025). The role of artificial intelligence in enhancing decision-making and efficiency in mergers and acquisitions: A case study approach within the U.S. capital market. *International Journal for Multidisciplinary Research (IJFMR), 7*(3). https://doi.org/10.36948/ijfmr.2025.v07i03.44171

Narteh-Kofi, E., Sampson, E., Hattoh, E., Akingbade, R., & Agbeve, V. (2025, July 30). Optimizing target identification in the U.S. capital market mergers and acquisitions through artificial intelligence: Implications for financial efficiency, compliance, and national economic competitiveness. *International Journal for Multidisciplinary Research (IJFMR), 7*(4). https://doi.org/10.36948/ijfmr.2025.v07i04.51702

Neoaz, N. (2025). Harnessing Artificial Intelligence for Cybersecurity in Healthcare and Food Processing: A Review of Emerging Trends and the Role of Generative Models like ChatGPT. *Global Trends in Science and Technology, 1*(3), 144-162.

Nisioti, A., Mylonas, A., Yoo, P. D., & Katos, V. (2018). From intrusion detection to attacker attribution: A comprehensive survey of unsupervised methods. *IEEE Communications Surveys & Tutorials, 20*(4), 3369-3388.

Olatuyi, T. (2025). *Pragmatic Approaches to Data Breach Prevention: Strategies Employed by IT Managers* (Doctoral dissertation, Walden University).

Ozkan-Okay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cybersecurity solutions. *IEEe Access, 12*, 12229-12256.

Rezaiezadeh Roukerd, F., & Rajabi, M. M. (2024). Anomaly detection in groundwater monitoring data using LSTM-Autoencoder neural networks. *Environmental Monitoring and Assessment, 196*(8), 692.

Salama, R., Altrjman, C., & Al-Turjman, F. (2024). Healthcare cybersecurity challenges: a look at current and future trends. *Computational intelligence and Blockchain in complex systems,* 97-111.

Sani, Z. N., & Aryee, B. A. (2025). Optimizing drug supply chains to prevent shortages in rural U.S. hospitals. *EPRA International Journal of Economics, Business and Management Studies.* https://doi.org/10.36713/epra24022

Soe, Y. N., Feng, Y., Santosa, P. I., Hartanto, R., & Sakurai, K. (2019). Rule generation for signature-based detection systems of cyber attacks in IoT environments. *Bulletin of Networking, Computing, Systems, and Software, 8*(2), 93-97.

Umoren, J., Korang, A., Utomi, E., Adukpo, T. K., Mensah, N. (2025). The Importance of Utilizing Big Data Analytics in U.S. Healthcare Supply Chain Management. *EPRA International Journal of Multidisciplinary Research, 11*(3), 411-421. https://doi.org/10.36713/epra20572

Umoren, J., Utomi, E., & Adukpo, T. K. (2025). AI-powered predictive models for U.S. healthcare supply chains: Creating AI models to forecast and optimize supply chain. *EPRA International Journal of Multidisciplinary Research (IJMR).* https://doi.org/10.36713/epra22481

Wang, Q., Su, M., Zhang, M., & Li, R. (2021). Integrating digital technologies and public health to fight the COVID-19 pandemic: key technologies, applications, challenges, and outlook of digital healthcare. *International Journal of Environmental Research and Public Health, 18*(11), 6053.

Yaqoob, T., Abbas, H., & Atiquzzaman, M. (2019). Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review. *IEEE Communications Surveys & Tutorials, 21*(4), 3723-3768.

Zhang, X., & Saltman, R. (2022). Impact of electronic health record interoperability on telehealth service outcomes. *JMIR medical informatics, 10*(1), e31837.

Zhang, Z., Al Hamadi, H., Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable artificial intelligence applications in cybersecurity: State-of-the-art in research. *IEEe Access, 10*, 93104-93139.