Sarcouncil Journal of Engineering and Computer Sciences

ISSN(Online): 2945-3585

Volume- 04| Issue- 10| 2025

Research Article **Received:** 11-09-2025| **Accepted:** 08-10-2025 | **Published:** 21-10-2025

The Role of Advanced Machine Learning Algorithms in Detecting and Mitigating Cybersecurity Threats within United States Healthcare Digital Infrastructure: A Comprehensive Vulnerability Analysis

Zeliatu Ahmed[1], Aisha Mohammed Suleiman[2], Abimbola Filani[3], Isaiah Thompson Ocansey[4] and Alice Ama Donkor[5]

[1]*Department of Information Systems, Cybersecurity, Dakota State University, Madison, USA*
[2]*University of Iowa, Iowa, USA*
[3]*Department of Business Information Systems, Central Michigan University, Michigan, USA*
[4]*University of Texas at El Paso*
[5]*Department of Computer Science, Kwame Nkrumah University of Science and Technology, Ghana*

Abstract: With rapid digitization within the United States healthcare sector, the dangers of cybersecurity threats are continuously combated using advanced machine learning (ML) algorithms. Cybersecurity in the healthcare industry faces a daunting set of challenges as data breaches become increasingly more sophisticated and traditional security measures fail to adequately protect sensitive patient data and critical healthcare systems. ML-driven systems have emerged with significant advantages to protecting critical healthcare systems including real-time threat detection, anomaly identification and predictive analytics, enhancing the overall resilience of a healthcare digital infrastructure. Nonetheless, despite these benefits, challenges of data privacy, algorithm bias and deployment complexities arise and need to be addressed to ensure reliability and ethical applications of ML technologies. The research work discusses the role of advanced machine learning (ML) algorithms in the detection and prevention of cybersecurity threats in healthcare systems. Through an extensive analysis of existing literature, this research examines how machine learning techniques such as deep learning, anomaly detection, and reinforcement learning improve defense through threat intelligence, intrusion detection and response. The findings reveal that anomaly detection models and deep learning frameworks greatly outperform the traditional rule-based systems for the detection of threats and behavioral anomalies in healthcare networks. Additionally, adaptive cybersecurity models that learn from novel attack patterns are increasingly utilizing reinforcement learning to induce systems that respond to attacks more proactively. However, despite these advances, there are still persistent gaps in terms of model interpretability, ethical governance, and deployment in real-world settings faced with heterogeneity of hospitals, emphasizing the need of regulatory frameworks and human-in-the-loop approaches. The findings offer valuable insights on how the U. S. healthcare security posture can be strengthened to build resilience against cybersecurity threats, while contributing to knowledge of the role of artificial intelligence approaches to securing healthcare digital infrastructure.

Keywords: Machine Learning, Cybersecurity, Healthcare Digital Infrastructure, Threat Detection.

INTRODUCTION

The rise of electronic health records (EHRs) and interoperable medical devices is ushering in a new digital era for healthcare. The aim of this shift is to provide enhanced patient care, better operational efficiency and improve data management. But as healthcare systems are getting increasingly digitized, the growing dependence on digital health infrastructure has placed health care organizations at risk for a wide range of cybersecurity vulnerability (Li, *et al.*, 2022). The increasing use of cloud-based medical records connected Internet of Medical Things (IoMT) devices, and telemedicine services have further expanded the attack surface, making the healthcare sector a key target for cybercriminals. Ransomware attacks on hospitals have caused operational disruptions, delayed treatments, and even compromised patient safety. Cybersecurity professionals have identified that one of the reasons healthcare systems are frequent victims of breaches, is particularly because they tend to have outdated security protocols in place with their networks which are not properly segmented and a lack of real-time detection systems. The healthcare industry also deals with aggravated issues of insider threats, with unauthorized access of medical data still one of the leading causes of healthcare data breaches (Schrader, 2025).

The increasing magnitude of these threats has resulted in greater demand for machine learning (ML) based cybersecurity solutions. Traditional security measures like rule-based firewalls and signature-based intrusion detection systems, often fall short in protecting against advanced cyber threats that evolve constantly. By analyzing huge volumes of data and finding anomalies suggesting a potential cyber threat, machine learning provides a proactive and adaptive approach to cybersecurity within healthcare. Machine learning-based security systems can detect threats in real time, quickly responding to anomalous network behavior to minimize the damage from attacks before they

***Corresponding Author:** Alice Ama Donkor

DOI- https://doi.org/10.5281/zenodo.17415316

escalate. Several studies have shown the utility of ML algorithms in detecting healthcare digital infrastructure attacks such as ransomware, phishing attacks and advanced persistent threats. Nonetheless, despite the potential benefits of using ML in managing digital healthcare infrastructure, some challenges such as data privacy, poor accuracy, and the need of extensive computational resources for its widespread and effective real-world adoption needs to be focused on (El-Sofany, *et al.*, 2024).

Although there has been a surge of information and research on the use of ML in various aspects of cybersecurity, few have focused on the actual vulnerabilities still existing in the healthcare ecosystem and the extent of effective use of ML algorithm to mitigate such risks. Malicious actors keep iterating through more sophisticated attack vectors, which take advantage of legacy systems configurations, weak access controls and unencrypted medical records. Cyber threats, which are evolving and dynamic in nature, require security measures which can predict, and eliminate potential attacks Initiates before they can cause harm (Patel, *et al.*, 2020). ML-based cybersecurity solutions offer an enhanced and more efficient approach to safeguarding digital healthcare assets by leveraging extensive datasets in detecting anomalies, predicting attack patterns, and enhancing real-time threat responses. Yet, these solutions carry their own limitations such as the quality and diversity of the training data used, their ability to differentiate normal and malicious activities within complex healthcare networks, and mitigation of false positives that could lead to interruptions in critical medical processes (Yussuf, *et al.*, 2024). In addition, there are growing concerns about data privacy, regulatory compliance, and ethical concerns associated with AI-driven monitoring, which contribute to the discussions surrounding the incorporation of ML into digital healthcare systems. Although ML algorithms have demonstrated impressive success in enhancing threat detection and response capabilities, their use in healthcare settings can be more complex and requires a delicate balance between security, privacy, and system efficiency. With the healthcare sector increasingly dependent on digital infrastructure, the responsibility of developing resilient ML-enabled security frameworks will be essential in protecting patient information and maintaining the integrity of overall healthcare services (Paul, *et al.*, 2023).

CYBERSECURITY THREATS IN U.S. HEALTHCARE DIGITAL INFRASTRUCTURE

Digitization is associated with susceptibility to evolving cyberattacks. As IoMT and interlinked healthcare technologies are in use, security within healthcare becomes even more complex. According to Burns, et al. (2016), the use of connected devices in today's healthcare system, from virtual diagnostic platforms to delivery and monitoring tools such as infusion pumps and implantable cardiac defibrillators, has introduced new cyber risks within healthcare, particularly making it vulnerable to ransomware attacks. Also, weak firewall configurations and little cybersecurity awareness amongst healthcare workers have created a conducive environment where phishing and malware threats are prevalent (Aljohani, 2022). These devices are often run by obsolete software or do not have strict security protocols and can be manipulated to obtain unauthorized access to a hospital's network or even manipulate patient care. Parmar (2012) highlights that devices such as insulin pumps for patients with diabetes are hacked easily and hence demonstrates that risks are inherent when it comes to digital medical devices.

Publisher: SARC Publisher

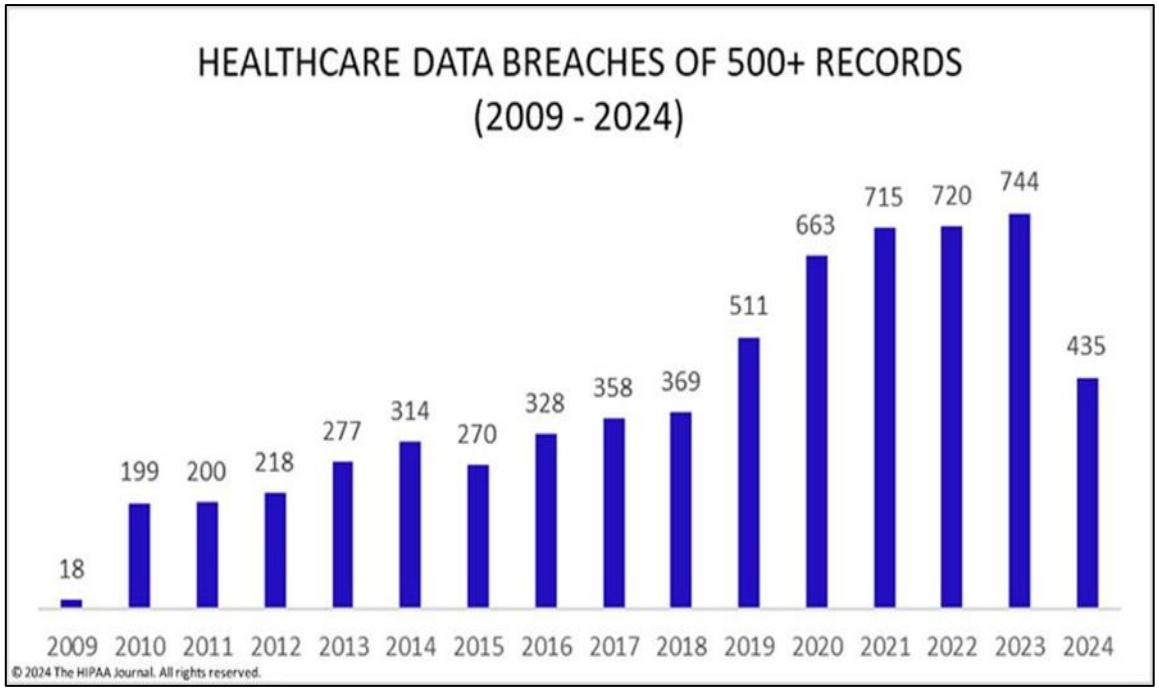

Figure 1: List of Healthcare Data Breaches (HIPAA Journal, 2024)

Third-party cybersecurity risks within healthcare may also arise from dependence on third-party suppliers, contractors, and external service providers that have access to sensitive patient data and critical systems. These risks include susceptibilities in cloud-based electronic health records (EHRs), supply chain attacks targeting manufacturers of medical devices and intrusions via third-party billing or telehealth platforms. According to the 2023 Health 3rd Party Trust Initiative (Health3PT) which is an entity made up of different bodies which includes the Health Information Trust Alliance (HITRUST), they reported 55% of healthcare organizations were victims of a third-party incident in 2023 (The HIPAA Journal, 2024). These incidents were considered third-party leaks of personally identifiable information (PII) and other protected health information.

On the other hand, mobile health and telemedicine are new spaces with new cybersecurity challenges. The healthcare industry's expansion into telemedicine has introduced its further exposure to cyberattacks since remote access security protocols are usually underdeveloped. According to Kotz, *et al.*, (2016), employing the public health service (PHS) to transfer health information through potentially inconvenient networks increases the risk of interception and uncontrolled access. Furthermore, the usage of personnel-owned portable devices in accessing patient information poses significant security risks and risks of compromise of patient data since these gadgets may not have the necessary security configurations which can expose patient data to leakage and potential violations and regulatory sanctions of these organizations in incidents where these devices are stolen.

Results shown by surgical retrieval demonstrate that security of healthcare organizations continues to weaken as they pursue better interconnectivity and data exchange between connected services. According to Walker (2017), interoperability standards allow the healthcare industries to accomplish implementing better and more quality patient care, although at the same time, it challenges security of health information throughout numerous systems and institutions. The challenges lie in managing connectivity requirements to enable the transfer of data and the difficulties of developing secure systems to meet the needs of patient privacy and the security of health care information systems.

Fig. 2 below shows the breakdown of vulnerabilities by age, with the categories being Recent, Moderate, and Older, for 3 critical sectors namely energy, water, and healthcare. This distribution reveals how infrastructure ages impact the occurrence of vulnerabilities and where mitigative actions should focus. In healthcare, moderate-age vulnerabilities predominate, indicating vulnerabilities old enough to be exploited but lacking full remediation strategies.

Publisher: SARC Publisher

Fig. 2. Vulnerability Age Distribution by Sector (Obioha-Val *et al.*, 2024)

Fig. 3 yields radar plots that compare the severity, exploitability, and vulnerability age across clusters, with the relative intensity of each characteristic being visualized. Cluster 1 shows ow severity with moderate exploitability which indicates moderate risk vulnerabilities. On the other hand, cluster 2 reveals high severity with medium exploitability and older age, indicating legacy vulnerabilities that, even though have not been exploited yet, still potentially pose considerable risk. The highest severity and recent age are exhibited in Cluster 3, represent a new high-risk vulnerabilities, warranting urgent response, especially in sectors such as healthcare where high-severity vulnerabilities are being reported.

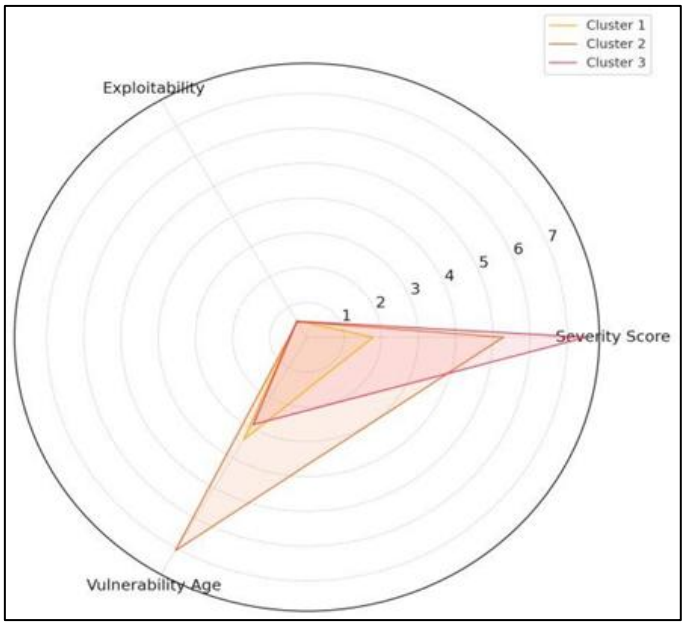

Fig. 3. Radar Plot of Vulnerability Characteristics Across Clusters (Obioha-Val *et al.*, 2024)

Publisher: SARC Publisher

In response to the evolving threat landscape, the U.S. government has implemented various healthcare cybersecurity resilience initiatives. Due to a recent devastating cyberattacks, a new bipartisan bill has been introduced in the U.S. to strengthen cybersecurity across healthcare and the public health sectors. This bipartisan bill known as the Healthcare Cybersecurity Act is required to direct the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Health and Human Services (HHS) to jointly work on enhancing healthcare cybersecurity and make necessary resources available to non-federal entities about cyber threats indicators and appropriate defenses (Industrial Cyber, 2024).

Additionally, with the Health Insurance Portability and Accountability Act (HIPAA) as a baseline regulation, healthcare organizations must appropriately implement policies and very strict security measures to protect electronic protected health information (ePHI). Also, the Health Information Technology Economic and Clinical Health Act (HITECH) further builds on those protections by increasing enforcement and breach notification requirements, so organizations take action to protect themselves against cyber threats. Additionally, the National Institute of Standards and Technology (NIST) Cybersecurity Framework outlines a set of risk management best practices that have been widely adopted across different sectors, including healthcare, to help them build resilient cybersecurity approaches. Despite these regulatory measures, many of these initiatives tend to be more reactive in nature, promoting compliance, reporting, and remediation after an event, instead of preventing cyber threats before they happen. As cyber threats continue to advance, like ransomware attacks that impede smooth hospital operations or AI-driven phishing attacks, the need for more proactive defenses and stringent measures becomes urgent. Incorporating advanced machine learning models that can detect anomalies in real time, provide predictive analytics, and facilitate automated threat responses would play a crucial role in transitioning the healthcare industry from a reactive cybersecurity approach to a proactive posture (Graham, 2024)

IMPACTS OF CYBERTHREATS ON US HEALTHCARE

The urgency to improve and enhance cybersecurity defenses is evidenced by quantitative data. According to Riel (2024), critical infrastructure such as healthcare worldwide experienced over 420 million cyber incidents from January 2023 to January 2024, which is an average of 13 attacks per second. On the economic front, cyberattacks are costly. The 2024 average ransomware recovery cost per incident neared $2.73 million, intensifying the hit to the economy from operational downtime. Employee susceptibility to phishing continues to also remain high, with 34.3% of employees being identified as vulnerable in 2023. Odo (2024) highlights that targeted and focused training proves effective to reducing this susceptibility, indicating how enhancing knowledge can contribute to building resilience amongst an organization's workforce against cyberattacks.

THE ROLE OF MACHINE LEARNING ALGORITHMS IN US HEALTHCARE CYBERSECURITY

AI technologies provide new avenues in automation or anomaly detection in healthcare security. Machine Learning (ML) has risen as an effective tool in contributing to secured healthcare. ML algorithms are good at examining large amounts of data produced by interconnected medical devices to detect anomalies that could point to potential security threats. The introduction of Machine learning (ML) in 5G networks has proven that ML techniques are very efficient in predicting and identifying cyber threats in various digital platforms.

Hussain *et al*., (2021) and Santhi, *et al*., (2021) emphasize the significance that machine learning (ML) plays in securing the Internet of Medical Things (IoMT), by proving the effectiveness of different approaches such as k-Nearest Neighbors (KNN), Support Vector Machines (SVM) and deep learning architectures, to detect cyber threats. Their studies emphasize the capabilities of these models to detect and prevent attacks with remarkable precision, reporting high accuracy rates of over 99% in some cases. A deep neural network was introduced by Vijayakumar et al. (2023) tailored for the detection of cyberattacks within health care environments, which achieved an impressive accuracy of 99.85%. Through the significant improvement of threat detection and reducing false positives, their model outperformed existing detection systems and highlights the potential of deep learning in strengthening cybersecurity within the healthcare sector. Their study highlights the increasing feasibility of using AI-driven security solutions to combat advanced cyberattacks in healthcare.

Publisher: SARC Publisher

IBM Watson is an AI-powered platform built to enhance threat detection and response capability in healthcare organizations by leveraging natural language processing and machine learning. It has the capacity to analyze large volumes of unstructured data, for instance, threat intelligence reports and cybercrime strategies, to spot emerging threats and offer actionable insights on how to address them. This cognitive method, with its focus on enabling real-time insights of potential threats, makes it easier for healthcare institutions to take effective and timely responses to cyber incidents. In addition, Watson's machine learning capabilities allow it to adapt to the evolving threat landscape and provide robust safeguards against increasingly sophisticated cyberattacks (Arefin and Simcox, 2024).

In a recent research study, a deep learning algorithm was developed by Liu, *et al.*, (2018), utilizing both reinforcement learning (LSTM networks) and supervised learning (CNN) to predict the occurrence of diseases, including heart failure, kidney failure, and stroke. This algorithm, unlike other prediction models, uses both structured data from EHR and unstructured data in progress and diagnosis notes. Thus, the inclusion of unstructured data within the model achieved a considerable improvement in all baseline metrics, highlighting the versatility and efficiency of such algorithms (Lui, *et al.*, 2018).

Moreover, another study by McKinney, *et al.*, (2020) implemented a deep learning algorithm to detect tumors in their earlier stages based on mammograms. Compared with traditional screening methods used for detection of tumors, these deep learning-based screen detection approaches allowed for the detection and location of the tumors at much earlier stages of breast cancer, giving a much better rate resection. When compared directly, this deep learning-based method outperformed experienced radiologists by an AUC score of 11.5%. Several other approaches have also developed ML-driven techniques for breast cancer detection with varying degrees of success, such as models developed by Wang, *et al.*, (2018) and Amrane, *et al.*, (2018).

The success of these ML-driven approaches suggests the crucial role that intelligent threat detection systems play in enhancing the security posture of healthcare and IoMT. These findings further emphasize the importance of embedded advanced machine learning models for early detection and analysis of any malicious activities in the healthcare ecosystem considering the growing sophistication of cyber threats targeting IoMT.

CHALLENGES AND LIMITATIONS OF ML IN HEALTHCARE DIGITAL INFRASTRUCTURE

While machine learning–based applications within healthcare offer novel and progressive opportunities, they also introduce unique risk factors, challenges, and warranted skepticism. Based on a probabilistic distribution, one of the biggest risks of machine learning-based algorithms is the probability of error in diagnosis and prediction. This also brings about a healthy skepticism about the validity and veracity of predictions from ML-based approaches (Cseko & Tremaine, 2013).

Another risk linked to applying ML and deep learning algorithms to healthcare is the availability of high-quality training and testing data with sufficiently large sample sizes to achieve high reliability and reproducibility of their predictions. As the ML and deep learning-based approaches are designed to learn from data, the significance of quality data is highly important. Also, the large amounts of feature-rich nature of data needed for these learning networks and approaches is not easily available and may also have a limited distribution of the population sample. Furthermore, in many healthcare segments, the collected data is partially unstructured, heterogeneous, and has significantly higher features compared to the number of samples (Finlayson, *et al.*, 2019).

A significant challenge in the application of ML approaches to healthcare is the interpretation and clinical relevance of the outputs. Because of the complex structure of ML-based approaches, especially deep learning-based methods, it becomes extremely challenging to separate and detect the contribution of the original features toward the prediction. While this may not be of major worry in other applications of ML like web searches, the lack of transparency has formed a major roadblock for the adoption of ML based methods in healthcare (Levine, *et al.*, 2019).

It is expected and currently being observed that as new technologies enter the scene, they are sure to come with new ethical dilemmas emerge (Mathiesen & Broekman, 2022). Various experts have argued that ethical dilemmas arising from ML algorithms may fall within domains of accountability, resource allocation equity, and

Publisher: SARC Publisher

personal integrity (Mathiesen & Broekman, 2022). Generalizations based on such algorithms can make low and middle-income countries particularly vulnerable due to bias. This is because of the lack of legal protection, predominance of bias against some minority groups and a lack of technical capacity (Fletcher, *et al.*, 2020). Therefore, there is a need for research to be focused on finding ethical dilemmas and develop guidelines to propose solutions to these ethical dilemmas.

FUTURE DIRECTIONS & CONCLUSION

The future of machine learning (ML) and deep learning in health care healthcare security depends on addressing data-centric challenges in quality, availability, and security perspectives. Given the dependence of these models on large, feature-rich datasets for accurate threat detection, the lack of comprehensive and representative data presents a major limitation. Tackling these gaps calls for a unified approach to standardizing the collection and enhancement of storage mechanisms and the use of advanced algorithms that can handle the processing of fragmented and unstructured data. The increasing focus on open science and collaborative sharing of biological data has the potential to vastly improve ML efficacy, but it also risks compromising ethical principles for patient privacy and data security. The sensitive nature of healthcare information requires very strict security protocols, especially as cloud-based infrastructures are common with ML implementations. To safeguard patient data, proactive measures must be taken to establish more robust encryption, access controls, and adherence to regulatory frameworks like HIPAA and the HITECH Act.

In addition, not only is the success of ML in healthcare security dependent on technological innovations. It needs to be practically integrated within healthcare systems. However, a systematic transition must be established between data science and clinical practice, to ensure that ML models become interpretable, explainable and align with security needs in the real world. The involvement of healthcare professionals in the development and validation of ML-based cybersecurity solutions can improve trust and adoption rates, facilitating seamless integration into existing healthcare workflows. Also, explainable AI (XAI) techniques can be used to augment ML interpretability so stakeholders can develop greater confidence in the automated decisions of security systems and pave the way for its adoption in practice. Future work should be focused on improving ML g algorithms to reduce false-positive and false-negative so as to ensure security interventions can be accurate and effective. Additionally, for its contribution to broader healthcare accessibility, ML can also address the cost of diagnostic tools and improve the security of telemedicine. Overcoming these challenges, while also utilizing technological innovations will enable the integration of ML into healthcare more seamlessly and efficiently, allowing for a more secure and efficient digital healthcare system.

REFERENCES

1. Burns, A. J., Johnson, M. E., & Honeyman, P. "A brief chronology of medical device security." *Communications of the ACM* 59.10 (2016): 66–72.
2. Alder, S. "2024 Healthcare Data Breach Report." *HIPAA Journal* (2025). https://www.hipaajournal.com/2024-healthcare-data-breach-report/
3. Parmar, A. "Hackers show off vulnerabilities in wireless insulin pumps." *Med City News* (2012). https://medcitynews.com/2012/03/hacker-shows-off-vulnerabilities-of-wireless-insulin-pumps/
4. Obioha-Val, O., Kolade, T. M., Gbadebo, M., Selesi-Aina, O., Olateju, O., & Olaniyi, O. "Strengthening Cybersecurity Measures for the Defense of Critical Infrastructure in the United States." *Asian Journal of Research in Computer Science* 17 (2024): 25–45. doi:10.9734/ajrcos/2024/v17i11517.
5. Kotz, D., Gunter, C. A., Kumar, S., & Weiner, J. P. "Privacy and security in mobile health: A research agenda." *Computer* 49.6 (2016): 22–30.
6. Walker, T. "Interoperability is a must for hospitals, but it comes with risks." *Managed Healthcare Executive* (2017). http://managedhealthcareexecutive.modernmedicine.com/managed-healthcare-executive/news/interoperability-must-hospitals-it-comes-risks
7. Industrial Cyber. "US senators introduce Healthcare Cybersecurity Act to boost sector's defenses against cyberattacks." *Industrial Cyber* (2024). https://industrialcyber.co/medical/us-senators-introduce-healthcare-cybersecurity-act-to-boost-sectors-defenses-against-cyberattacks/

Publisher: SARC Publisher

8. Graham, E. *Methodology for assessing information security of third-party risk management in healthcare organizations.* PhD Thesis, University of Colorado Colorado Springs, 2024. ProQuest Dissertations & Theses, 31765886.
9. Riel, J. F. "Examining the Implications of a Significant Cyberattack on U.S. Infrastructure." *Encompass* (2024). https://encompass.eku.edu/honors_theses/1044/
10. Odo, C. "Strengthening Cybersecurity Resilience: The Importance of Education, Training, and Risk Management." *Social Science Research Network* (2024).
11. Arefin, S., & Simcox, M. "AI-Driven Solutions for Safeguarding Healthcare Data: Innovations in Cybersecurity." *International Business Research* 17.6 (2024): 1-74.
12. Liu, J., Zhang, Z., & Razavian, N. "Deep EHR: Chronic disease prediction using medical notes." *arXiv* (2018): arXiv:1808.04928.
13. Fakhouri, H. N., Alawadi, S., Awaysheh, F. M., Imad, B. H., Alkhalaileh, M., & Hamad, F. "A comprehensive study on the role of machine learning in 5G security: Challenges, technologies, and solutions." *Electronics* 12.22 (2023): 4604.
14. Hussain, F., Abbas, G. S., Shah, A. G., Pires, M. I., Fayyaz, U. U., Shahzad, F., et al. "IoT healthcare security dataset." *IEEE Dataport* (2021).
15. Santhi, J., & Saradhi, T. V. "Attack detection in medical Internet of Things using optimized deep learning: Enhanced security in healthcare sector." *Data Technologies and Applications* 55.5 (2021): 682–714.
16. Vijayakumar, P. K., Pradeep, K., Balasundaram, A., & Prusty, R. M. "Enhanced cyber attack detection process for Internet of Health Things (IoHT) devices using deep neural network." *Processes* 11.4 (2023): 1072.
17. McKinney, S. M., Sieniek, M., Godbole, V., Godwin, J., Antropova, N., Ashrafian, H., et al. "International evaluation of an AI system for breast cancer screening." *Nature* 577.7788 (2020): 89–94.
18. Cseko, G. C., & Tremaine, W. J. "The role of the institutional review board in the oversight of the ethical aspects of human studies research." *Nutrition in Clinical Practice* 28.2 (2013): 177–181.
19. Finlayson, S. G., Bowers, J. D., Ito, J., Zittrain, J. L., Beam, L., & Kohane, I. S. "Emerging vulnerabilities demand new conversations." *Science* 363.6433 (2019): 1287–1290. doi:10.1126/science.aaw4399.
20. Levine, D. M., Linder, J. A., & Landon, B. E. "Characteristics of Americans with primary care and changes over time, 2002–2015." *Annals of Internal Medicine* 169.1 (2019): 36–43. doi:10.1001/jamainternmed.2019.6282.
21. Wang, D., Li, J. R., Zhang, Y. H., Chen, L., Huang, T., & Cai, Y. D. "Identification of differentially expressed genes between original breast cancer and xenograft using machine learning algorithms." *Genes (Basel)* 9.3 (2018): 1–16.
22. Amrane, M., Oukid, S., Gagaoua, I., & Ensar, İ. T. "Breast cancer classification using machine learning." *Electric Electronics, Computer Science, Biomedical Engineerings' Meeting (EBBT)* (2018): 1–4.
23. Fletcher, R. R., Nakeshimana, A., & Olubeko, O. "Addressing fairness, bias, and appropriate use of artificial intelligence and machine learning in global health." *Frontiers in Artificial Intelligence* 3 (2020): 561802.
24. Mathiesen, T., & Broekman, M. "Machine learning and ethics." *Acta Neurochirurgica Supplement* 134 (2022): 251–256.
25. Li, E., Clarke, J., Ashrafian, H., Darzi, A., & Neves, A. L. "The impact of electronic health record interoperability on safety and quality of care in high-income countries: Systematic review." *Journal of Medical Internet Research* 24.9 (2022): e38144. doi:10.2196/38144.
26. Schrader, D. "A comprehensive guide to healthcare cybersecurity." *Netwrix Blog* (2025). https://blog.netwrix.com/healthcare-cybersecurity#:~:text=71%25%20of%20respondents%20reported%20that,be%20attributed%20to%20several%20factors
27. El-Sofany, H., El-Seoud, S. A., Karam, O. H., & Bouallegue, B. "Using machine learning algorithms to enhance IoT system security." *Scientific Reports* 14.1 (2024): 12077. doi:10.1038/s41598-024-62861-y.
28. Patel, N. M., Schirm, J., & Lakhani, S. "Safeguarding the digital hospital: Cybersecurity in the age of rapid technological advancement." *American Journal of Roentgenology* 214.6 (2020): 1235–1241.
29. Yussuf, M., Lamina, A., Mesioye, O., Nwachukwu, G., & Aminu, T. "Leveraging Machine Learning for Proactive Threat Analysis in Cybersecurity." *International Journal of Computer Applications Technology*

Publisher: SARC Publisher

and Research 13 (2024): 53–64. doi:10.7753/IJCATR1309.1005.
30. Paul, M., Maglaras, L., Ferrag, M. A., & Almomani, I. "Digitization of healthcare sector: A study on privacy and security concerns." *ICT Express* 9.4 (2023): 571–588. doi:10.1016/j.icte.2023.02.007.

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
Ahmed, Z., Suleiman, A. M., Filani, A., Ocansey, I. T. and Donkor, A. A. "The Role of Advanced Machine Learning Algorithms in Detecting and Mitigating Cybersecurity Threats within United States Healthcare Digital Infrastructure: A Comprehensive Vulnerability Analysis." *Sarcouncil Journal of Engineering and Computer Sciences* 4.10 (2025): pp 218-226.

Publisher: SARC Publisher