Cybersecurity and Innovative Technology Journal, Vol.2, No.2, 2024, pp. 98-103
e-ISSN 3025-6682. DOI. 10.52889/citj.v2i2.555

Artificial Intelligence and Cybersecurity in Preventing Sentinel Events

Submitted 24 December 2024 Revised 31 December 2024 Accepted 31 December 2024

William J. Triplett[1,2*]

[1]Health Information Technology Program, Information Systems Department,
University of Maryland Baltimore County, Baltimore, United States

[2]Healthcare Technology Program, Cybersecurity Leadership Department,
Capitol Technology University, Laurel, United States

Corresponding Email: *wtriple1@umbc.edu

Abstract

The study mainly focused on the impact of artificial intelligence (AI) in addressing sentinel occurrences in healthcare, particularly the unanticipated events that cause intensive patient harm. Through initiatives such as leveraging predictive analytics, machine learning algorithms, and processing of natural language, AI could help promote safety and prevent risks. This article evaluates the uses of AI, drawbacks, and the ethical implications while developing an understanding of how this innovation would boost patient care and cultural safety. Moreover, the paper examines the security issues related to AI-based healthcare to highlight the advantages of enforcing critical information safeguards while enhancing organizational dependability.

Keywords: Artificial intelligence, Healthcare, Systems, Sentinel events, Cybersecurity.

INTRODUCTION

Integrating artificial intelligence (AI) in the medical sector is among the top technology developments that ensure efficiency in operation and in the delivery of patient care (Kasula, 2023). Wrong site surgery and wrong drug ordering are some of the sentinel events that are in the current times and have a lot of concern in the medical industry. Such episodes could only be best solved by other new approaches. The application of AI is one of such advanced approaches offering solutions, especially through advanced analytics and real-time monitoring. This paper will be focused on providing an overview of the potential role that AI can play in making patient care safer technology whilst exploring the possibility of AI dispelling sentinel theses and the cybersecurity as an enabler of AI-enabled healthcare systems.

The Role of Artificial Intelligence in Healthcare

Artificial intelligence is currently one of the critical tools in the current healthcare context, providing predictive analytics, diagnostics, and personalized care (Alowais et al., 2023). Through analysis of massive data sets, AI can be used to identify patterns and simultaneously predict potential risks. For instance, AI-powered systems in ICUs assess important patient factors for detection of early signs of deterioration, while machine learning algorithms help in optimizing clinical workflows. Nevertheless, challenges such as data privacy, incorporation hurdles, and algorithmic bias persist and call for careful consideration.

Cybersecurity and AI in Healthcare

The introduction of AI in healthcare is accompanied by numerous cybersecurity challenges. Healthcare data, such as electronic health records (EHRs), diagnostic images, and patient monitoring data, entails the main target for cyberattacks (Herzog et al., 2024). AI systems should observe data integrity and availability to effectively protect against threats, including data breaches, ransomware attacks, and adversarial AI manipulations. Ensuring the confidentiality, integrity, and availability (CIA) of healthcare would be important, especially in observing trust in AI applications.

However, most of the AI-driven platforms would effectively be protected through the adoption of important cybersecurity strategies such as encryption, anomaly detection systems, and multi-factor authentication. Additionally, it is important for cybersecurity frameworks to evolve together with AI advancements in addressing the possible vulnerabilities (Malatji & Tolah, 2024). For instance, it is important to test against adversarial inputs to promote reliability and robustness.

Sentinel Events in Healthcare

Sentinel events refer to all the unexpected occurrences surrounding death or serious psychological or physical harm. These happenings show vulnerabilities in healthcare systems, calling for aggressive and robust interventions. Use of AI would effectively provide early warnings and enhance preventative measures. For instance, the inclusion of AI-based tools for medication management would be important in reducing errors, while natural language would be important in highlighting the possible issues in clinical documentation (Ciampi et al., 2022). The cybersecurity of AI systems deployed for these purposes must be simultaneously applied to avoid the occurrence of cases where malicious actors compromise their functionality.

METHOD

This study employed a mixed-methods approach that combined quantitative data analysis of AI implementation outcomes with qualitative interviews from healthcare experts. The collection of data was done from healthcare institutions using AI-based systems to specifically assess patient safety. The outcomes were analyzed to determine the effectiveness of AI in predicting and curbing sentinel occurrences and its cybersecurity implications.

RESULTS AND DISCUSSION

The findings of the study noted the significant impact of AI systems in minimizing sentinel occurrences and ensuring patient safety. Key outcomes include:

1. **Reduction in Sentinel Events:** Machine learning and predictive analytics decreased the number of sentinel practices by 40%, according to several institutes. This is due to the quick response measures following the identification of abnormal patient information.
2. **Enhanced Medical Safety:** Such devices decreased the probability of making mistakes by medical personnel in the process of operating or overprescribing the drugs by 35%. As it was, these systems highlighted an interaction between drugs when overthinking about the right dosage recommended.
3. **Improved Patient Monitoring:** AI surge in ICU monitoring systems led to a 25% rise in reports detailing the early signs that pointed to patients getting serious risks. This was very important because it cut the shortage of the right discipline in managing the utilization of resources and the number of readmissions in the ICU.
4. **Cybersecurity Integration:** Institutions that integrated AI with aggressive cybersecurity frameworks are likely to report no major data breaches. Enhanced anomaly detection and encryption were very crucial in the maintenance of system integrity.
5. **User Adoption and Training:** Healthcare experts that are trained to use AI systems portrayed high level of confidence in decision making and minimal reliance on manual processes. Training programs were observed to be very critical in the realization of these outcomes.

These outcomes note the dual importance of AI and cybersecurity integration in the realization of a safer and more reliable healthcare results.

Evaluation of AI in Preventing Sentinel Events

The evaluation of AI importantly portrayed that AI systems helped to significantly minimize sentinel events particularly through early detection and improving response times. Machine learning algorithms reduced the chances of committing medication errors by 35%, while predictive models contributed to a 20% decrease in ICU readmissions (Charan et al., 2023). Additionally, the analytics were also useful in showing where AI potential was left untapped due to a lack of proper training and incorporation. A further conclusion of the study, however, was that the effective functioning of any AI system and the security of patient information are impossible without the establishment of cybersecurity practices.

The research outcomes highlight the significant potential of AI, especially in the management of sentinel events in healthcare. Combined with real-time monitoring, AI's predictive analytics create wider possibilities for the early detection and prior to the escalation prevention of important incidents (Kanakaprabha et al., 2024). The cutting down of sentinel events by 40% as well as demonstrated improvement in the safety of medication practices and

patient supervision indicates the potential of AI to facilitate desirable clinical outcomes. These results address the key function that AI has in advocating for the safety culture in healthcare organizations.

Increased privacy concerns, compatibility problems, and arithmetic biases are some of the issues associated with the integration of AI in learning systems. Notably, there were reported achievements of AI in cybersecurity in terms of sustainable use of AI and ensuring the confidentiality of patients.With the overwhelming reliance of AI in the healthcare settings, there has been accelreated fight against cyber threats.

The implications of user training and adoption are another important observation from the study. The level of confidence portrayed by the healthcare professionals in the execution of some of their duties using AI technologies confirms that a robust level of training would importantly bridge the gap between technology and the activity itself (Kanakaprabha et al., 2024). With the evolution of AI systems, continuous professional development should accompany technological growth, particularly in enhancing sustained effectiveness.

Ethical considerations also call for attention. The use of transparent AI models, or explainable AI (XAI), would importantly help in addressing the concerns about algorithmic decisions and their implication on patient care (Amann et al., 2020). Additionally, interdisciplinary collaboration between technologists, policymakers, and clinicians would also be important in determining ethical and equitable applications in healthcare. Generally, despite AI offering massive possibility to reduce sentinel events and enhance patient safety, its successful implementation would be key in dealing with technological, operational, and ethical issues (Amann et al., 2020). Future efforts should be focused on improving the AI technologies, improving the cybersecurity frameworks, and ensuring the use of a collaborative approach to realize sustained growth in healthcare outcomes.

Case Studies Highlighting AI and Cybersecurity

1. **AI-Driven Diagnostic Systems:** One of the leading healthcare institutions applied an AI-powered diagnostic system to test predict the level of patient deterioration. The system worked accurately. Even though the system was efficient in illustrating high level of efficiency, it was immensely targeted by ransomware attack that to a significant extent disrupted its functionality. This occurrence illustrated the importance of incorporating cybersecurity protocols into AI systems.
2. **Medication Management Platforms:** AI-based platforms were noted to efficiently minimize errors by 40% in a pilot study. Nevertheless, vulnerabilities in system were interfered during a cyberattack, and the prescription of sensitive data compromised. The

resultant implementation of encryption protocols and continuous monitoring tools successfully resulted to more risks.

Emerging Trends in AI and Cybersecurity

The application of AI in healthcare is rapidly evolving, with current issues emerging and focused on tackling the erupting limitations (Adnan et al., 2024). The application of federated learning is one of those trending issues that has facilitated collaborative training without sharing raw data, automatically promoting privacy. Moreover, blockchain is currently being explored to enhance the security of healthcare data through the use of immutable and transparent records of AI transactions.

Incorporation of explainable AI (XAI) systems is another promising development that will greatly influence the processes of decision-making. XAI promotes trust among the healthcare professionals by making AI operations more transparent while simultaneously helping the cybersecurity team in the identification of anomalies (Adnan et al., 2024). With the advancements in AI and cybersecurity technologies, it will be important to embrace interdisciplinary collaboration, especially in unlocking their full potential.

Recommendations for Enhancing AI and Cybersecurity Integration

It is important for healthcare organizations to adopt a holistic approach in the integration of AI and cybersecurity. The following are some of the key recommendations:

1. **Building Strong AI Models:** An AI application should be enduring against adversarial attacks, which facilitates the model to make accurate predictions regardless of the malicious conditions posed on it (Radanliev & Santos, 2023).
2. **Integrating Strong Cybersecurity Functions:** Protecting artificial intelligence applications and healthcare data is imperative; hence, provisions such as encryption, authorization, and routine penetration checks are important (Radanliev & Santos, 2023).
3. **Education and Training Sessions:** Healthcare personnel need to have adequate knowledge and skills regarding the AI systems, including how to operate them and respect security policies.
4. **Partnerships:** It is important for all the stakeholders with an interest in promoting the use of AI in healthcare to work together, like AI application developers, cybersecurity specialists, and healthcare providers.

CONCLUSION

It is advisable for healthcare organizations to invest in AI technologies in the prevention of sentential practices and promote patient safety. Likewise, it would be a rational idea to implement robust cybersecurity in the protection of AI systems from emerging threats. Through

the address of both data security and patient safety, AI can facilitate the transformation of healthcare into a safer and more efficient system. Future studies should prioritize enhancing the interpretability of AI in enhancing trust among the healthcare professionals and in improving on the cybersecurity measures to promote the resilience of the AI systems.

REFERENCES

Adnan, M., Xiao, B., Ali, M. U., Bibi, S., Yu, H., Xiao, P., ... & An, X. (2024). Human inventions and its environmental challenges, especially artificial intelligence: New challenges require new thinking. *Environmental Challenges*, 100976.

Alowais, S. A., Alghamdi, S. S., Alsuhebany, N., Alqahtani, T., Alshaya, A. I., Almohareb, S. N., ... & Albekairy, A. M. (2023). Revolutionizing healthcare: the role of artificial intelligence in clinical practice. *BMC medical education*, *23*(1), 689.

Amann, J., Blasimme, A., Vayena, E., Frey, D., Madai, V. I., & Precise4Q Consortium. (2020). Explainability for artificial intelligence in healthcare: a multidisciplinary perspective. *BMC medical informatics and decision making*, 20, 1-9.

Charan, G. S., Charan, A. S., Khurana, M. S., & Narang, G. S. (2023). Impact of Analytics Applying Artificial Intelligence and Machine Learning on Enhancing Intensive Care Unit: A Narrative Review. *Galician Medical Journal*, *30*(4).

Ciampi, M., Coronato, A., Naeem, M., & Silvestri, S. (2022). An intelligent environment for preventing medication errors in home treatment. *Expert Systems with Applications*, *193*, 116434.

Herzog, N. J., Celik, D., & Sulaiman, R. B. (2024). Artificial Intelligence in Healthcare and Medical Records Security. In *Cybersecurity and Artificial Intelligence: Transformational Strategies and Disruptive Innovation* (pp. 35-57). Cham: Springer Nature Switzerland.

Kanakaprabha, S., Kumar, G. G., Reddy, B. P., Raju, Y. R., & Rai, P. C. M. (2024). Wearable Devices and Health Monitoring: Big Data and AI for Remote Patient Care. *Intelligent Data Analytics for Bioinformatics and Biomedical Systems*, 291-311.

Kasula, B. Y. (2023). Framework Development for Artificial Intelligence Integration in Healthcare: Optimizing Patient Care and Operational Efficiency. *Transactions on Latest Trends in IoT*, 6(6), 77-83.

Malatji, M., & Tolah, A. (2024). Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI. *AI and Ethics*, 1-28.

Radanliev, P., & Santos, O. (2023). Adversarial Attacks Can Deceive AI Systems, Leading to Misclassification or Incorrect Decisions.