International Journal of Recent Advances in Multidisciplinary Topics
Volume 6, Issue 4, April 2025
https://www.ijramt.com | ISSN (Online): 2582-7839

Utilizing AI to Fortify Physical and Cyber Security in Hospitals

Shashank Sambamoorthy[1], Sambamoorthi Subramaniam[2*]
[1]Cyber Security Practitioner & Strategist, Orlando, USA
[2]SME-Cyber Security, VCISO, Chennai, India

***Abstract*: The emergence of Generative Artificial Intelligence (AI) applications represents a gamechanger with profound opportunities and risks. AI applications span across every industry, from automating repetitive tasks to accelerating discoveries in healthcare and science.**

***Keywords*: Artificial Intelligence, Applications, Cyber Security, Gamechanger, Health care, Hospitals, Health Insurance Portability and Accountability Act, HIPAA, Physical security,**

1. Introduction

This article explores the list of opportunities for utilizing AI applications in a hospital environment to fortify physical and cyber security.

A. Cybersecurity Opportunities with AI

AI offers a more agile and intelligent approach to security compared to traditional rule-based systems by continuously learning and adapting to new patterns of behavior. Here are a few opportunities to strengthen cyber security posture with AI.

1. Automated threat detection is a key benefit, with AI tools monitoring network activity 24/7 to identify suspicious behaviors like abnormal data transfer spikes or unauthorized access attempts, drastically reducing response times
2. *Network Security*: AI can identify vulnerabilities across various endpoints, including medical equipment, administrative systems, and patient portals, allowing IT teams to address issues proactively.
3. *Incident Response*: AI can assist by isolating compromised systems, containing threats, and initiating remediation protocols, ensuring business continuity.
4. *Threat Identification*: AI can help identify and mitigate threats like ransomware by monitoring unusual file access or encryption activity.
5. Phishing attacks can be detected through AI analysis of email metadata, content, and language patterns.
6. Predictive analytics for cybersecurity enables AI to analyze historical data and identify patterns to forecast potential vulnerabilities and recommend proactive security measures, preventing attacks before they happen.
7. Data masking techniques using AI can reduce the risk of personal health information (PHI) exposure in datasets used for analysis and testing.
8. *Audit Logs*: AI can automatically create and maintain detailed audit logs of data access and modifications, ensuring transparency and accountability as required by HIPAA.
9. Continuous risk assessments can be conducted by AI by analyzing data and identifying potential vulnerabilities.
10. *Real-Time Alerts*: AI can provide real-time alerts for potential HIPAA violations, enabling swift action to mitigate risks.
11. *Third-Party Vendor (TPV)*: AI can assist in managing third-party vendors by monitoring their activities to ensure HIPAA compliance and alerting to potential issues.
12. *Data Encryption*: AI can enhance data encryption by automatically applying advanced encryption algorithms to secure sensitive healthcare information and adapt protocols to emerging threats.
13. AI can be used to recognize patterns and detect anomalies associated with attacks and fraud, leading to faster identification of suspicious activities and potential breaches.
14. AI can continuously monitor user behavior to detect anomalies indicative of insider threats, such as unusual logins or data transfers.
15. AI can help healthcare organizations fully leverage AI to identify vulnerabilities and misconfigurations, detect suspicious activities, contain attacks, prioritize remediation, and generate compliance documentation.
16. *HIPAA Compliance*: AI systems can monitor network traffic and identify unusual patterns that may indicate a data breach or unauthorized access, aiding in anomaly detection for HIPAA compliance

By implementing these AI-powered solutions, hospitals and healthcare facilities can significantly enhance their security posture, protect patient data, ensure regulatory compliance, and improve overall safety for patients, staff, and visitors. However, it's crucial to address ethical considerations, ensure transparency, and implement appropriate safeguards to mitigate potential risks associated with AI adoption.

*Corresponding author: saamba@gmail.com

2. Physical Security Enhancements through AI

1. Facial recognition can be used to identify and alert staff to persons of interest, provide biometric access control for staff, and aid in targeted evidence searching.
2. Loitering detection tracks individuals and can trigger events like lighting, sounds, or staff notifications if someone stays in an area for an extended period, helping to distinguish between casual waiting and potentially criminal intent.
3. *Fall Prevention*: AI-powered solutions can contribute to fall prevention by notifying staff when a patient leaves their bed, attempts to do so, has been out of bed longer than expected, or has fallen, enabling a timely response.
4. *Detect Firearms*: AI-integrated camera systems can help detect firearms and provide notifications when weapons are spotted, enhancing the ability to identify and respond to threats.
5. *Ambient Sounds*: AI systems can analyze ambient sounds, such as screaming in a waiting room, and alert security personnel to potential disturbances9.
6. *Video Analytics*: AI-powered video analytics and computer vision improve overall security strategies by leveraging the capabilities of video surveillance systems.

3. Conclusion

The new age of AI has ushered in new era that requires a paradigm shift in the way we lead and manage change. The acceleration of change requires that we learn, adapt, adjust, and develop new mental frameworks faster than we used to. The above is the indicative list of opportunities where the power of AI can be utilized to enhance the physical and cybersecurity posture of a hospital and healthcare clinics.

References

[1] ways healthcare facilities are using AI-powered video surveillance solutions, by Brian T. Horowitz, https://healthtechmagazine.net/article/2023/12/how-hospitals-are-adopting-artificial-intelligence-safeguard-patients-staff

[2] Matthew Kjin, "5 ways healthcare facilities are using AI-powered video surveillance solutions," March 3, 2025 https://newsroom.axis.com/blog/ai-video-surveillance-healthcare
AI and Machine Learning in De-identifying Healthcare Data: Future Trends and Applications, June 11 2024, https://imerit.net/blog/ai-and-machine-learning-in-de-identifying-healthcare-data-future-trends-and-applications/

[3] Using AI Threat Detection in Healthcare – Clear DATA, March 7, 2025,

[4] https://www.cleardata.com/blog/using-ai-threat-detection-in-healthcare/?utm_medium=Social-Organic&utm_source=Twitter&utm_campaign=Strategic-Cost-Cutting

[5] Tshidiso Makhene, "Using AI for HIPAA compliance" July 24, 2024. https://www.paubox.com/blog/using-ai-for-hipaa-compliance

[6] https://ambient.ai/solutions/healthcare

[7] Khan, M.M., Alkhathami, M. Anomaly detection in IoT-based healthcare: machine learning for enhanced security. Sci Rep 14, 5872 (2024).

[8] Cyber Security for healthcare organizations, Point of View (POV), https://healthtechmagazine.net/article/2023/12/how-hospitals-are-adopting-artificial-intelligence-safeguard-patients-staff