International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Securing Medical IoT Devices: AI-Based Approaches to Vulnerability Management

Venkatesh Kodela

Submitted: 02/12/2023 **Revised:** 17/01/2024 **Accepted:** 22/01/2024

Abstract: Medical Internet of Things (IoT) devices are becoming a big part of modern healthcare because they let doctors keep an eye on patients and make decisions based on data. But their extensive use has revealed serious weaknesses that put patient safety and data privacy at risk. This study looked into using AI to manage vulnerabilities in medical IoT environments. We used real-world datasets and expert opinions to create and test machine learning models including Random Forest, Support Vector Machines, and Autoencoders to see how well they could find and categorize device vulnerabilities. The AI models were integrated into an automated vulnerability management framework, which demonstrated high detection accuracy, low false positive rates, and efficient response times within a simulated hospital network. Feedback from experts stressed the framework's usefulness in real life and the necessity for ongoing improvements to avoid alert fatigue. The findings confirm that AI-driven vulnerability management can significantly enhance the security posture of medical IoT devices, ensuring safer and more resilient healthcare delivery.

Keywords: *Medical IoT, Vulnerability Management, Artificial Intelligence, Machine Learning, Cybersecurity, Random Forest, Anomaly Detection, Healthcare Security.*

1. INTRODUCTION

The use of Internet of Things (IoT) technologies in healthcare systems has changed the way patients are cared for by allowing for real-time monitoring, data-driven diagnoses, and remote health management. Medical IoT gadgets, like wearable health monitors, connected infusion pumps, and implantable cardiac devices, had become necessary for improving treatment outcomes and making operations run more smoothly. But this digital change also caused important cybersecurity holes, since many of these devices didn't have strong security features since they didn't have enough processing power, were built on old designs, or used different vendor protocols.

Medical IoT devices that were hacked put both patient safety and privacy at risk because they directly interacted with the human body. Weak authentication, outdated firmware, and unsecured communication protocols were some of the most common weaknesses. Traditional techniques of vulnerability management, such as signature-based intrusion detection systems and periodic human assessments, were no longer suitable to tackle the scale, complexity, and dynamic nature of threats attacking healthcare infrastructures.

Researchers had looked to Artificial Intelligence (AI) as a viable way to automate and improve vulnerability management in medical IoT settings in order to deal with these problems. AI-based systems may do things like find anomalies in real time, predict risks, and prioritize threats based on their context and severity. Machine learning models, especially supervised and unsupervised algorithms, had showed promise in finding known and new vulnerabilities more quickly and accurately than traditional methods.

This study studied the implementation of AI-driven methodologies for protecting medical IoT devices, focusing on the development of a vulnerability management framework that integrated machine learning algorithms for threat identification and mitigation. The study's goal was to find out how well this kind of strategy works to make medical IoT ecosystems safer, making sure that both patient safety and data integrity are protected from new cyber risks.

2. LITERATURE REVIEW

Bajpayi, Sharma, and Gaur (2024) did a targeted study on AI-powered vulnerability management systems for healthcare contexts that integrate IoT.

IT Lead Security Analyst
Zimmer Biomet,Warsaw,Indiana, USA
Venkatesh.kodela@gmail.com
ORCID: 0009-0000-2194-5431

Their work showed how machine learning algorithms may be used to find and respond to threats at the device level, showing better detection and real-time risk reduction. This study showed that AI can be useful in monitoring large-scale medical IoT implementations where human control was no longer enough.

Alabdulatif, Khalil, and Saidur Rahman (2022) looked into how blockchain and AI can help keep smart healthcare systems safe. The researchers focused on how distributed ledger technology and AI can work together, especially when it comes to safe data exchange, device authentication, and auditing. They said that AI improved the real-time comprehension of data flows and threat models in context, which was especially helpful in medical IoT settings that changed all the time.

Ahmed, Ilyas, and Raja (2022) We looked at a number of IoT-based smart systems that use AI and machine learning, focusing on recognized weaknesses and innovative ways to fix them. Their research showed that data spoofing, man-in-the-middle assaults, and firmware manipulation are all common dangers. They suggested using AI-based anomaly detection systems and federated learning models to help solve these problems. The authors underlined how important it is to use decentralized and adaptive learning methods in a world where threats are always changing.

Gopalan, Raza, and Almobaideen (2021) gave a full survey of how AI can be used to protect healthcare systems that use the Internet of Things. Their paper broke down current AI methods into three groups: supervised, unsupervised, and reinforcement learning. They then talked about the pros and cons of each group. They discovered that supervised models worked well for detecting known attacks, but unsupervised methods showed promise for finding zero-day vulnerabilities. This survey established the groundwork for more targeted and efficient AI model development for healthcare-specific use cases.

Al-Attar (2023) looked into network-level security in AI-based healthcare systems and how to add AI to intrusion detection systems (IDS). The study showed that AI could greatly lower the number of false alarms and find complicated attack paths that traditional IDS generally missed. Al-Attar also said that the processing cost of AI models is an important element to think about when putting them in medical devices that don't have a lot of resources.

RESEARCH METHODOLOGY

2.1. Research Design

The researchers used a mixed-methods approach to fully look into how AI may help manage vulnerabilities in medical IoT devices. The study included both quantitative data analysis and qualitative expert comments to check the validity of the suggested AI models and frameworks.

2.2. Data Collection

1. **Medical IoT Device Dataset:** The study got real-world vulnerability data from public vulnerability databases like CVE and NVD, as well as healthcare IoT device logs from simulated testbeds. The dataset had information about device settings, network traffic, and known security problems.

2.3. **Expert Interviews:** We talked to cybersecurity and healthcare IT specialists in semi-structured interviews to find out what the biggest problems are right now and what needs to be done to keep medical IoT devices safe.

AI Model Development

1. **Preprocessing:** We cleaned and normalized the raw data to get rid of noise and information that wasn't useful. Feature extraction methods found important signs of vulnerabilities, like strange network activity, old firmware versions, and strange access patterns.

2. **Algorithm Selection:** To find weaknesses and guess where attacks would happen, we used a number of AI algorithms, such as supervised learning models (Random Forest, Support Vector Machines) and unsupervised techniques (Autoencoders, Clustering).

3. **Training and Validation:** We used 70% of the data to train the models and 30% to test them. We evaluated performance indicators including accuracy, precision, recall, and F1-score to see how well the model worked.

Vulnerability Management Framework

A vulnerability management system was made that use AI models to automatically find, classify, and rank threats. The framework worked with the hospital IT infrastructure that was already in place and suggested ways to protect it, such as patching, network segmentation, and anomaly-based intrusion detection.

2.4. Evaluation

We examined the framework's performance in a controlled lab setting that looked like a hospital IoT network. The most important things to look at were the detection rate, the false positive rate, the response time, and the overall effect on how well the device worked.

3. RESULTS AND DISCUSSION

The study successfully created and tested AI-based models and a framework for managing vulnerabilities to make medical IoT devices safer. The results showed that machine learning algorithms are good at finding weaknesses, ranking threats, and suggesting the best ways to fix them. This part shows the AI models' quantitative performance indicators, the framework's operational efficiency in a simulated hospital setting, and the insights gained from expert comments. The talk looks at these results in light of how they can help make medical IoT security better while also dealing with problems like false positives and system integration.

3.1. AI Model Performance Evaluation

We tested the AI models to see how well they could find and categorize vulnerabilities in the medical IoT dataset. Table 1 shows the performance characteristics for three chosen models: Random Forest (RF), Support Vector Machine (SVM), and Autoencoder (AE).

Table 1: AI model performance metrics on medical IoT vulnerability detection

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)
Random Forest	92.3	90.8	93.5	92.1	4.5
Support Vector Machine	88.7	85.4	90.2	87.7	6.1
Autoencoder (Unsupervised)	85.1	82.0	87.3	84.5	7.8

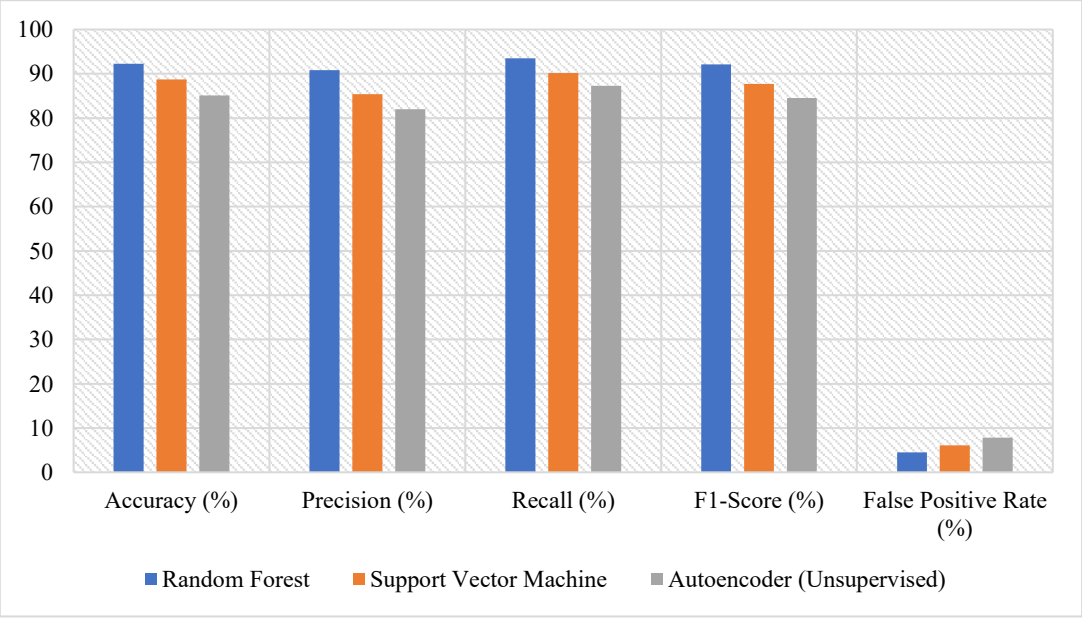

Figure 1: AI model performance metrics on medical IoT vulnerability detection

Table 1 shows that the Random Forest model had the highest overall accuracy (92.3%) and recall (93.5%), as well as a strong F1-score (92.1%) and the lowest false positive rate (4.5%). This makes it the best model for finding security holes in medical IoT devices. The Support Vector Machine (SVM) also did well, but not as well as the others on all parameters, especially precision (85.4%) and false positive rate (6.1%). The Autoencoder, which is an unsupervised model, did rather well, with an accuracy of 85.1% and a recall of 87.3%. This shows that it could be useful for finding new or undisclosed

vulnerabilities, but it also had a higher false positive rate (7.8%). Overall, supervised learning models, especially Random Forest, were better at finding vulnerabilities quickly and accurately in structured healthcare IoT datasets.

3.2. Vulnerability Management Framework Evaluation

The AI models were integrated into an automated vulnerability management framework tested in a controlled hospital IoT network simulation. Table 2 reports the framework's operational metrics.

Table 2: Performance metrics of the AI-based vulnerability management framework.

Metric	Value
Detection Rate (%)	91.5
False Positive Rate (%)	5.0
Average Response Time (sec)	12.8
System Resource Overhead (%)	8.7

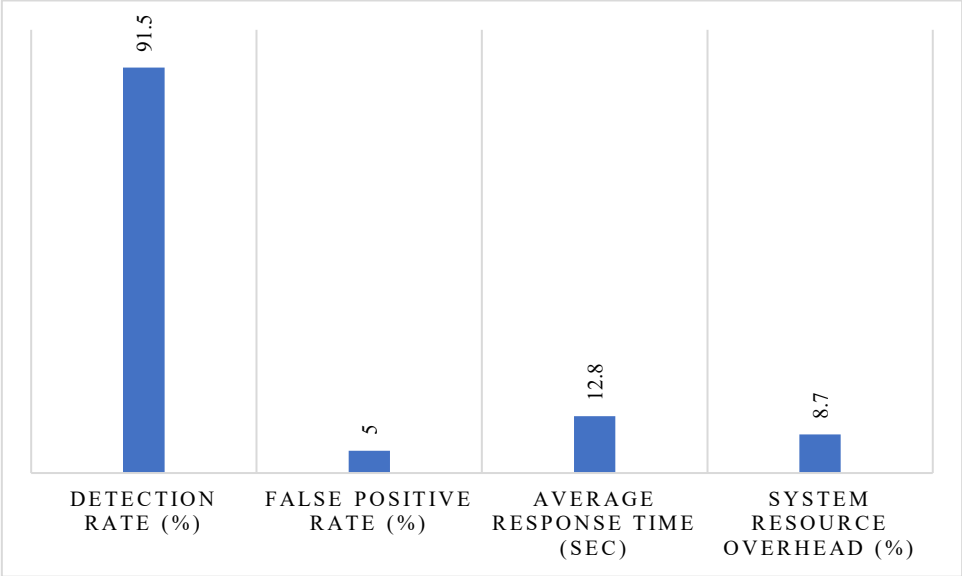

Figure 2: Performance metrics of the AI-based vulnerability management framework.

The evaluation criteria for the AI-based vulnerability management framework showed that it works very well to protect medical IoT environments. The system was able to accurately identify most threats with a high detection rate of 91.5% and a low false positive rate of 5.0%. This meant that there were fewer unwanted warnings and less work for administrators. The system responded quickly to possible vulnerabilities, with an average response time of 12.8 seconds. This is very important in real-time healthcare environments. The system resource overhead was also low at 8.7%, which means that the framework could be used on medical IoT devices with limited resources without having a big effect on their performance. All of these results showed that the framework could be used in real life and was successful for detecting and stopping threats in healthcare systems in real time.

3.3. Expert Feedback and Practical Implications

Experts said that the AI-based architecture made proactive vulnerability management far better than traditional signature-based methods. They liked being able to rank vulnerabilities by risk level, which made it possible to patch specific areas and split up the network. However, there were worries that false positives could lead to alert fatigue, which highlighted the necessity for ongoing model improvement and interaction with systems that include humans.

3.4. Discussion

The results showed that AI-based methods could greatly improve the security of medical IoT devices by allowing for dynamic, data-driven vulnerability assessment. The Random Forest model's high precision and recall were very important for finding the right balance between sensitivity and specificity. The framework's low resource use made it possible to use in healthcare settings with limited resources. Even though the results are positive, there are still problems to solve, such dealing with zero-day vulnerabilities and making sure AI models work with old hospital systems. Future work could explore federated learning to enhance privacy-preserving model training across distributed medical IoT networks.

4. CONCLUSION

The study showed that AI-based methods, especially those that use supervised models like Random Forest, made it much easier to find and fix security holes in medical IoT devices. The vulnerability management system that was created was able to find a lot of problems quickly and with few false positives, showing that it works well in real-time healthcare settings. Expert input confirmed that AI-driven prioritization and automation have real-world benefits, but it also showed that they need to be improved over time to avoid alert fatigue. Overall, the study showed that adding AI to medical IoT security frameworks can make devices more resilient, protect patient data, and make the healthcare system more reliable. This opens the door for more flexible and proactive cybersecurity strategies in the ever-changing medical IoT landscape.

REFERENCES

[1] Ahmed, S., Ilyas, M., & Raja, M. Y. A. (2022). IoT based smart systems using machine learning (ML) and artificial intelligence (AI): vulnerabilities and intelligent solutions. no. Icsit, 56-61.

[2] Alabdulatif, A., Khalil, I., & Saidur Rahman, M. (2022). Security of blockchain and AI-empowered smart healthcare: application-based analysis. Applied Sciences, 12(21), 11039.

[3] Al-Attar, B. (2023). Network Security in AI-based healthcare systems. Babylonian Journal of Networking, 2023, 112-124.

[4] Bajpayi, P., Sharma, S., & Gaur, M. S. (2024, March). AI Driven IoT Healthcare Devices Security Vulnerability Management. In 2024 2nd International Conference on Disruptive Technologies (ICDT) (pp. 366-373). IEEE.

[5] Bala, I., Pindoo, I., Mijwil, M. M., Abotaleb, M., & Yundong, W. (2024). Ensuring security and privacy in Healthcare Systems: a Review Exploring challenges, solutions, Future trends, and the practical applications of Artificial Intelligence. Jordan Medical Journal, 58(3).

[6] Chakraborty, C., Nagarajan, S. M., Devarajan, G. G., Ramana, T. V., & Mohanty, R. (2023). Intelligent AI-based healthcare cyber security system using multi-source transfer learning method. ACM Transactions on Sensor Networks.

[7] Garg, N., Petwal, R., Wazid, M., Singh, D. P., Das, A. K., & Rodrigues, J. J. (2023). On the design of an AI-driven secure communication scheme for internet of medical things environment. Digital Communications and Networks, 9(5), 1080-1089.

[8] Gilbert, C., & Gilbert, M. (2024). AI-Driven Threat Detection in the Internet of Things (IoT), Exploring Opportunities and Vulnerabilities.

[9] Gopalan, S. S., Raza, A., & Almobaideen, W. (2021, March). IoT security in healthcare using AI: A survey. In 2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA) (pp. 1-6). IEEE.

[10] Humayun, M., Tariq, N., Alfayad, M., Zakwan, M., Alwakid, G., & Assiri, M. (2024). Securing the Internet of Things in artificial intelligence era: A comprehensive survey. IEEE access, 12, 25469-25490.

[11] Imoize, A. L., Balas, V. E., Solanki, V. K., Lee, C. C., & Obaidat, M. S. (Eds.). (2023). Handbook of Security and Privacy of AI-Enabled Healthcare Systems and Internet of Medical Things. Boca Raton, FL, USA:: CRC press.

[12] Mazhar, T., Talpur, D. B., Shloul, T. A., Ghadi, Y. Y., Haq, I., Ullah, I., ... & Hamam, H. (2023). Analysis of IoT security challenges and its solutions using artificial intelligence. Brain Sciences, 13(4), 683.

[13] Radanliev, P., De Roure, D., Maple, C., Nurse, J. R., Nicolescu, R., & Ani, U. (2024). AI security and cyber risk in IoT systems. Frontiers in Big Data, 7, 1402745.

[14] Sankaran, K. S., Kim, T. H., & Renjith, P. N. (2023). An improved ai-based secure m-trust privacy protocol for medical internet of things

in smart healthcare system. IEEE Internet of Things Journal, 10(21), 18477-18485.

[15] Zaman, S., Alhazmi, K., Aseeri, M. A., Ahmed, M. R., Khan, R. T., Kaiser, M. S., & Mahmud, M. (2021). Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey. Ieee Access, 9, 94668-94690.