Mitigating Security Threats in Smart Devices Through Artificial Intelligence

Amrinder Singh[1], Dr. Saurabh Sharma[2]

Research Scholar[1], Associate Professor[2]

Department of Computer Science and Applications, Sant Baba Bhag Singh University

Amrindersing0008@gmail.com

How to Cite this Article:

Singh, A. (2026). Mitigating Security Threats in Smart Devices Through Artificial Intelligence. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.159

https://doi.org/ 10.55041/ijcope.v2i4.159

Abstract

The fast growth of Internet of Things (IoT) technologies and smart devices has changed modern life by authorizing connectivity, automation, and instant decision-making. However, this growth of technologies has introduced various major risks associated with cybersecurity due to the weak security mechanisms. Traditional security approaches are unable to address and solve the threats such as zero-day attacks, unauthorized access. Artificial Intelligence (AI) offers intelligent and real-time solutions that are able to detecting the threats and responding automatically. This research identifies the major security vulnerabilities in the smart devices and provide an AI-based framework for mitigating the cyber threats. The findings states that AI- driven system provide a higher accuracy in the detection and faster responses as compared to traditional methods. The research concludes that integrating AI into the smart devices is necessary for ensuring the long-term digital safety.

Keywords: Artificial Intelligence, Internet of Things, security mechanisms, Cybersecurity, Machine Learning, decision-making.

Introduction

Smart devices have now become a very crucial part of daily life, these are used in wide range of applications such as home automation, wearable healthcare, etc. Those devices constantly gather, process and transfer the data with the help of interconnected devices by improving the operational efficiency. Despite these benefits, their rapid adoption has significantly expanded the attack surface for cybercriminals. Most of the smart devices operate with limited processing memory and power, it also restricts the execution of strong security procedures. In addition, most of the devices are dependent on the unsecured wireless connections, default passwords many devices rely on default passwords, outdated firmware, and unsecured wireless connections, increasing the risk of cyber-attacks. As people are relying more on the smart devices the risk of privacy violation, financial loss and threat to public safety increases. There is a need of smart protective system.

Artificial Intelligence provides the advanced solutions in order to address these challenges. AI system is capable enough to analyse large amount of data, detect the unusual activities and responds to these threats.

This research focus on exploring how Artificial Intelligence can mitigate security threats in smart devices and provides a conceptual framework for protection.

2. Literature Review

Previous research highlights the growing importance of AI in cybersecurity for smart environments. Studies indicate that the proliferation of IoT devices has significantly increased vulnerabilities due to heterogeneous architectures and weak security standards.

According to M Brundage, S Avin

This report examines the possible security threats caused by the misuse of Artificial Intelligence (AI). It explores how AI can affect security in digital, physical, and political areas. The study also provides key recommendations for researchers and stakeholders to handle these threats. It suggests important areas for future research to improve defense systems and reduce the effectiveness of attacks. Additionally, the report discusses the ongoing balance between attackers and defenders. However, it does not provide a final conclusion on this issue.

According to S Zaman, K Alhazmi, MA Aseeri, MR Ahmed

The Internet of Things (IoT) connects devices, people, and systems to improve daily life. These devices often have limited power and memory, making them vulnerable to cyberattacks. Traditional security methods are not always effective for protecting IoT networks. Strong encryption is difficult to apply due to resource constraints in devices. Artificial Intelligence (AI), including machine learning, can enhance security by detecting threats. This study explores IoT security challenges, AI-based solutions, and future research directions.

According to Y Hu, W Kuang, Z Qin

In recent years, Artificial Intelligence (AI) has rapidly developed and is widely used in areas such as education, healthcare, finance, and image recognition, often outperforming humans in many tasks. However, AI systems are vulnerable to various security threats at different stages, including data collection, training, and deployment. These threats include sensor spoofing, data poisoning, and adversarial attacks. Therefore, it is important to apply strong security measures throughout the entire lifecycle of AI systems. This study reviews the major security challenges and available solutions in AI. It also highlights future challenges and opportunities to improve AI security.

According to H Wu, H Han, X Wang, S Sun

The Internet of Things (IoT) has developed through authentication, communication, and computing, creating many smart solutions for different applications. However, due to its open nature and limited resources, IoT faces various security threats at each layer. This study reviews the complex security challenges in IoT systems. It highlights that Artificial Intelligence (AI), including Machine Learning and Deep Learning, can help improve IoT security. The paper also discusses AI-based solutions for major threats like device authentication, DoS/DDoS attacks, intrusion detection, and malware detection. Finally, it points out that AI also brings new challenges and suggests future research directions to address them.

According to S Ahmed, MF Hossain

Smart cities have developed with the growth of information and communication technology and advanced sensing systems. They use sensors to collect data and improve services like transport, healthcare, water supply, and environmental monitoring. This data helps manage urban systems efficiently and provide better services to people. Machine learning and cloud-based technologies further improve efficiency by reducing resource usage. However, these systems also raise serious concerns about security and privacy, as connected devices are vulnerable to cyberattacks. This study discusses these security issues and explains AI-based solutions for protecting smart city applications like health, transport, and energy.

According to S Shahriar, S Allana

Artificial Intelligence (AI) and machine learning have become powerful tools used in many fields such as healthcare, finance, politics, and surveillance systems. These applications generate large amounts of data related to different aspects of human life. While AI provides many benefits, it also raises serious concerns about data privacy. Privacy risks can occur at different stages of the AI lifecycle, including data collection, processing, and usage. This study identifies key risks such as identity exposure, wrong decisions, lack of transparency, and non-compliance with privacy rules. It also reviews solutions, technologies, and policies to protect privacy and highlights future challenges in AI systems.

According to MA Khatun, SF Memon

Healthcare Internet of Things (H-IoT), also called digital healthcare, uses smart devices like sensors and monitors to improve diagnosis and treatment. These systems depend on data and connected devices for faster and better healthcare services. However, IoT devices are becoming more vulnerable to cyber threats, which can lead to data breaches and unauthorized access. This study discusses privacy and security challenges in healthcare IoT, especially related to machine learning. It also highlights the importance of monitoring different layers such as perception, network, cloud, and application. Finally, it explains the need for strong AI-based authentication and security methods to protect healthcare systems from cyber risks.

According to L Gudala, M Shaik

The rapid growth of the Internet of Things (IoT) has connected billions of devices that collect and share data across different areas. However, this connectivity also creates major security challenges, as many IoT devices have limited power and memory. These limitations make them easy targets for cyberattacks, and traditional security methods are often not enough. Artificial Intelligence (AI) helps improve security by detecting threats, identifying unusual behaviour, and responding quickly. This paper studies AI-based methods such as anomaly detection and machine learning for identifying cyber threats. It also explains how supervised and unsupervised learning can be used to detect both known and unknown attacks in IoT systems.

According to M Waqas, S Tu, Z Halim

Security is a major concern in networks and communications, especially with the rapid increase in wireless devices. Artificial Intelligence (AI) has emerged as an effective solution to tackle these challenges. This survey categorizes different security threats and explores how AI can address them. It provides a comprehensive review of AI-based solutions for various security issues. The study also highlights key findings, recent developments, and future research directions. Additionally, it discusses how AI can be better utilized to handle advanced and emerging security threats.

Overall, the literature confirms that AI provides significant advantages in detecting complex, unknown, and evolving cyber threats. However, challenges remain regarding computational efficiency, data quality, and system scalability.

3. Research Methodology

This study adopts a descriptive research design which was purely based in the secondary data sources. It involves following stages:

3.1 Data Collection

All the data and information were collected from the various research articles, journals, case studies and the reputed databases such as Google Scholar. Cyberattacks on the smart devices were also examined in the study.

3.2 Analysis of Security Threats

Common threats identified include:

- Malware and ransomware attacks
- Unauthorized access and device hijacking
- Data leakage and privacy violations
- Denial-of-Service (DoS) attacks
- Network spoofing and intrusion

These threats exploit weaknesses such as insecure communication channels, outdated software, and poor authentication mechanisms.

4. Proposed AI-Based Security Framework

The research proposes a layered framework for securing smart devices using AI.

4.1 Data Collection Layer

This layer gathers device logs, network traffic, and operational data to establish baseline behaviour patterns.

4.2 Data Preprocessing Layer

Raw data is cleaned, filtered, and transformed to remove noise and extract relevant features. Proper preprocessing improves model performance and reduces computational load.

4.3 AI Analysis Engine

The core component employs machine learning and deep learning models to detect anomalies and classify potential threats. The system continuously learns from new data, improving accuracy over time.

4.4 Intrusion Detection Module

This module monitors device activity in real time and identifies suspicious behaviour such as unusual network traffic or unauthorized access attempts.

4.5 Decision-Making Module

Based on threat severity, appropriate actions are determined, including blocking traffic, isolating compromised devices, or issuing alerts.

4.6 Security Response Layer

Implements defensive measures automatically to minimize damage and restore normal operation.

4.7 Monitoring and Feedback Loop

Continuous monitoring ensures that the system adapts to new threats through retraining and updates.

5. Results and Discussion

Analysis of existing studies indicates that AI-based security systems outperform traditional methods in several aspects.

- **Higher Detection Accuracy:** AI models can achieve detection rates above 90% in many scenarios.
- **Reduced False Alarms:** Behavioral analysis helps distinguish legitimate activities from attacks.
- **Real-Time Response:** Automated detection enables immediate action.

- **Zero-Day Attack Detection:** AI can identify previously unknown threats by recognizing abnormal patterns.
- **Scalability:** Suitable for large-scale smart environments such as smart cities and industrial IoT systems.

However, challenges include high computational requirements for deep learning models, the need for high-quality training data, and potential privacy concerns.

6. Conclusion

The rapid growth of smart devices has created unprecedented cybersecurity challenges that cannot be effectively addressed using traditional methods alone. This research demonstrates that Artificial Intelligence provides powerful tools for enhancing security through intelligent monitoring, anomaly detection, and automated response mechanisms.

The proposed AI-based framework offers a comprehensive solution for protecting smart devices against modern cyber threats. By leveraging machine learning and deep learning techniques, the system can detect both known and unknown attacks with high accuracy while maintaining real-time performance.

Future research should focus on implementing the framework in real-world environments, improving energy efficiency for resource-constrained devices, and addressing ethical and privacy issues associated with AI deployment. As smart technologies continue to evolve, integrating AI into cybersecurity strategies will be essential for ensuring safe and reliable digital ecosystems.

7. References

Ahmed, S., Hossain, M. F., Kaiser, M. S., Noor, M. B. T., Mahmud, M., & Chakraborty, C. (2021). Artificial intelligence and machine learning for ensuring security in smart cities. In *Data-driven mining, learning and analytics for secured smart cities: Trends and advances* (pp. 23-47). Cham: Springer International Publishing.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint arXiv:1802.07228*.

Gudala, L., Shaik, M., Venkataramanan, S., & Sadhu, A. K. R. (2019). Leveraging artificial intelligence for enhanced threat detection, response, and anomaly identification in resource-constrained iot networks. *Distributed Learning and Broad Applications in Scientific Research*, *5*, 23-54.

Hu, Y., Kuang, W., Qin, Z., Li, K., Zhang, J., Gao, Y., ... & Li, K. (2021). Artificial intelligence security: Threats and countermeasures. *ACM Computing Surveys (CSUR)*, *55*(1), 1-36.

Khatun, M. A., Memon, S. F., Eising, C., & Dhirani, L. L. (2023). Machine learning for healthcare-IoT security: A review and risk mitigation. *IEEE access*, *11*, 145869-145896.

Shahriar, S., Allana, S., Hazratifard, S. M., & Dara, R. (2023). A survey of privacy risks and mitigation strategies in the artificial intelligence life cycle. *IEEE Access*, *11*, 61829-61854.

Waqas, M., Tu, S., Halim, Z., Rehman, S. U., Abbas, G., & Abbas, Z. H. (2022). The role of artificial intelligence and machine learning in wireless networks security: Principle, practice and challenges. *Artificial Intelligence Review*, *55*(7), 5215-5261.

Wu, H., Han, H., Wang, X., & Sun, S. (2020). Research on artificial intelligence enhancing internet of things security: A survey. *Ieee Access*, *8*, 153826-153848.

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.