PHYTON-ANNALES REI BOTANICAE
ISSN: 0079-2047
Volume 66 No. 1 (2026)
https://phyton-annales.com

Cybersecurity in the Internet of Things: Threats, Vulnerabilities, and Solutions

Dr. Julien Morel
Centre for Artificial Intelligence Research,
Nouvelle Sorbonne Institute of Technology, France

Submission Date: 20.08.2025 | Acceptance Date: 01.11.2025 | Publication Date: 17.02.2026

Abstract:
With its ability to link anything from smart household appliances to industrial sensors, the Internet of Things (IoT) has quickly become an essential component of contemporary life. Despite the many benefits that the Internet of Things (IoT) brings in terms of automation, efficiency, and convenience, it also poses several cybersecurity risks. the security flaws and risks that come with Internet of Things (IoT) systems, with an emphasis on the particular dangers presented by the vast array of linked devices, which frequently have insufficient processing capacity and use antiquated security standards. Here we take a look at the most typical ways that hackers can get into the Internet of Things, such as data breaches, denial-of-service attacks, and unauthorised access. We also go over the security risks that might result from improperly configured devices, insufficient encryption, and outdated software. offers some answers to lessen these dangers, such as more secure communication protocols, better authentication methods, and edge computing. In addition, we examine how AI and ML can be used to detect and counteract security risks to the Internet of Things in real-time. Lastly, in order to guarantee the security and reliability of IoT ecosystems in a globally interconnected environment, it is crucial to implement thorough cybersecurity frameworks and laws.
Keywords: Cybersecurity, Internet of Things (IoT), IoT Security Threats, IoT Vulnerabilities, Data Breaches

Introduction

Quickly changing the way, we engage with our environment is the Internet of Things (IoT). Internet of Things (IoT) holds great potential to revolutionise several industries through the interconnection of billions of devices, from smart thermostats and wearable health monitors to industrial sensors and driverless vehicles. This promises to bring about significant improvements in efficiency, convenience, and innovation. Nevertheless, there are substantial cybersecurity concerns that arise from this interconnection. The proliferation of IoT devices increases the attack surface, giving bad actors more chances to penetrate systems by exploiting vulnerabilities. Many Internet of Things (IoT) devices lack the resources of typical computing systems, including storage, processing power, and energy, making them challenging to secure using conventional approaches. Weak security mechanisms, poorly configured devices, and inadequate protection against unwanted access are common outcomes of these limitations. Data breaches, privacy violations, and denial-of-service assaults are already serious problems, and

the Internet of Things (IoT) makes it much more difficult to apply uniform security controls to all devices and networks. the cybersecurity issues encountered by IoT systems, delving into the specific dangers and weak spots caused by the extensive usage of linked devices. We go over the most typical entry points for attackers, such as hacking, manipulating devices, and intercepting data, and we emphasise the possible repercussions of these security lapses. Strengthened authentication methods, secure communication protocols, and the incorporation of edge computing to improve security are some of the measures we suggest to lessen the impact of these threats. We also investigate how new technology, such as machine learning and artificial intelligence (AI), can help with real-time threat detection and response. In order to protect the authenticity, privacy, and integrity of linked environments, it is crucial to resolve the security issues that come with IoT as it develops and grows. With the world becoming more interconnected, this paper seeks to survey the present landscape of Internet of Things (IoT) cybersecurity, pinpoint critical weaknesses, and offer practical solutions to protect IoT ecosystems.

AI and Machine Learning in IoT Security

Traditional security solutions are facing serious problems from the ever-increasing volume, variety, and complexity of data produced by interconnected devices as the Internet of Things (IoT) grows. Machine learning (ML) and artificial intelligence (AI) are becoming potent weapons in the fight against these threats to the Internet of Things (IoT). Through the use of these technologies, IoT systems may bolster system resilience, react instantly to security problems, and increase threat detection.

1. Real-Time Threat Detection and Prevention

Manually monitoring and identifying threats is often a challenge in IoT networks due to the large number of devices involved and the dynamic nature of their operational settings. Automatic analysis of network traffic patterns and device behaviour can be done by AI and ML algorithms, with a focus on anomaly detection models, to spot suspicious actions that could be signs of security breaches. These models can detect anomalies, such suspicious data flows, illegal device access, or unexpected control orders, in real-time. They are trained on massive datasets of typical system behaviour. Eliminating the window of opportunity for attackers and reducing the likelihood of severe security breaches are both made possible by this ability to detect and respond to threats instantly.

In smart home systems, for instance, security solutions powered by AI can spot suspicious communication patterns among devices, including when someone gains access to smart locks or when sensors or cameras do something unexpected. Immediate notifications and automated responses, including contacting the homeowner or locking down the compromised device, are made possible by this.

2. AI-Based Intrusion Detection Systems (IDS)

To find and stop intruders from getting into IoT networks, Intrusion Detection Systems (IDS) are essential. In order to identify new or complex assaults, traditional intrusion detection systems (IDS) use predefined signatures or criteria. Machine learning, on the other hand, may

adjust its detection methods to new forms of threats that may not have been previously noticed by continuously learning from incoming data.

Unsupervised learning algorithms, such as clustering and anomaly detection models, can detect outliers and possible dangers without requiring labelled datasets, whereas supervised learning techniques, like decision trees and support vector machines, can categorise benign and harmful traffic patterns. Artificial intelligence-powered intrusion detection systems are useful for protecting IoT networks from both current and future threats because of their capacity to learn and adapt on their own.

3. Automating Response to Security Incidents

Both the detection of threats and the automation of reactions to security incidents can be facilitated by AI and ML. When a security breach occurs in a conventional system, it takes human intervention to determine what happened and how to fix it. On the other hand, systems powered by AI can respond to threats automatically, without any human intervention, drastically cutting down on attack mitigation time and damage.

For instance, when AI detects an intrusion in an industrial IoT system, it can immediately isolate the compromised device, restrict harmful traffic, and begin security protocols like software patches or re-authentication. In large-scale networks, where human intervention is typically impossible, this automated response helps keep IoT devices secure even when no one is immediately watching.

4. Enhancing Authentication and Access Control

Internet of Things (IoT) authentication methods can also benefit from machine learning techniques. Attempts at brute-force authentication or credential theft are two threats that traditional authentication techniques like passwords and PINs face. Through the use of adaptive authentication methods, behavior-based analysis, or biometric authentication, machine learning has the potential to enhance security.

To illustrate the point, ML systems may track user and device interactions and trends over time to build a personalised profile. The system has the ability to lock down access or initiate an extra authentication step if a device or user tries to perform something that goes against their usual behaviour. Behaviour biometrics is a method that greatly improves the security of Internet of Things (IoT) devices' access control mechanisms.

5. Predictive Security and Vulnerability Management

Patching and vulnerability management are two examples of proactive security methods that utilise machine learning. Machine learning algorithms can examine attack data and system weaknesses to determine which networks or devices will be attacked by cybercriminals. The Internet of Things (IoT) can then prioritise fixing security holes and bolstering defences before an assault even happens.

In order to foretell potential dangers, AI systems can also study patterns in attack techniques and new security concerns. Organisations can lessen the chances of successful attacks by implementing preventive measures after they have a good grasp of the ever-changing world of IoT security.

With its ability to identify threats in real-time, automate responses, and improve authentication processes, AI and ML are quickly becoming crucial components of IoT security. These

solutions enhance the security and resilience of IoT networks by constantly learning from data and adjusting to new threats. With the proliferation of the Internet of Things (IoT), the security of linked systems is becoming more important, and the incorporation of artificial intelligence (AI) and machine learning (ML) is going to play a pivotal role in meeting these issues.

Conclusion

Thanks to the new age of networked gadgets brought about by the Internet of Things (IoT), many industries are now more efficient, convenient, and automated than ever before. Nevertheless, in order to safeguard sensitive information and guarantee the reliability of interconnected settings, major cybersecurity concerns posed by IoT systems are becoming more pressing as their size and complexity increase. the most important dangers that may compromise the security of the Internet of Things, such as unauthorised access, data breaches, DoS attacks, and the dangers that come with poorly configured devices. Securing IoT systems is particularly challenging due to the heterogeneous and resource-constrained nature of IoT devices, necessitating often tailored solutions to adequately reduce risks. Additionally, we have investigated a number of options for bolstering the security of the Internet of Things, including the use of robust authentication methods, encrypted communication protocols, and edge computing to process data more efficiently. Machine learning and artificial intelligence have also been very helpful in identifying and countering attacks in real-time, which has increased the security of IoT networks. It is essential that makers and consumers of IoT devices embrace thorough cybersecurity standards, adhere to best practices, and remain educated about new dangers as the network grows. With the right safeguards in place, the Internet of Things (IoT) can keep bringing about its revolutionary promise while reducing threats to people's personal information and physical safety. In the future, a crucial factor in ensuring the security of IoT ecosystems will be the integration of IoT security with cutting-edge technologies such as 5G, AI, and blockchain. To guarantee that the advantages of the Internet of Things (IoT) are achieved without jeopardising security or user confidence, we need to create security solutions that are both more resilient and more flexible.

Bibliography

Singh, A., & Chen, Y. (2023). *Threat Landscape Modeling for IoT Networks.* Journal of Cyber Defense Systems, 15(2), 112–129.

Martínez, L., & Okoye, T. (2024). *Vulnerability Assessment Frameworks for Smart Devices.* International Journal of IoT Security, 9(1), 45–61.

Tanaka, H., Al-Farsi, R., & Müller, I. (2023). *Lightweight Encryption Protocols for Resource-Constrained IoT Devices.* IEEE Transactions on Secure Computing, 8(4), 256–270.

Kobayashi, S., & Osei, H. (2022). *A Comparative Study of Intrusion Detection Techniques in IoT Environments.* Journal of Network Security Engineering, 12(3), 183–198.

Ahmed, S., & Petrescu, E. (2024). *Machine Learning-Driven Anomaly Detection in Smart Home Networks.* Journal of Intelligent Security Systems, 7(1), 79–95.

Rinaldi, M., & Velázquez, M. (2023). *Blockchain-Based Authentication for IoT Ecosystems.* International Journal of Distributed Ledger Security, 10(2), 87–103.

Ndlovu, T., & Suzuki, K. (2022). *Resilient Firmware Update Mechanisms for IoT Devices.* Cybersecurity and Trust Journal, 6(4), 201–215.

Hassan, L., & Dlamini, S. (2023). *Risk Mitigation Strategies for Industrial IoT Systems.* Journal of Industrial Cybersecurity, 11(1), 50–68.

Gupta, P., & Zhao, M. (2024). *Adaptive Security Frameworks Using Edge Computing for IoT Protection.* International Review of Edge-Based Security, 4(3), 134–150.

Novak, E., & Farid, R. (2022). *Secure Data Transmission Protocols for Wearable IoT Devices.* Journal of Embedded System Security, 5(2), 29–47.