IoT Security: Attacks, Security Tools, Machine Learning and Frameworks

Jozef Fiala[1], Slavomír Tatarka[1], Jozef Papán[1], Michal Kvet[1], Jan Panuš[2]

Abstract – The rapid proliferation of Internet of Things (IoT) devices has brought significant advancements across various sectors, yet their widespread use exposes them to numerous cybersecurity risks. This article comprehensively analyses IoT cybersecurity, focusing on common attack vectors, defensive mechanisms, and analytical tools. Key threats such as device spoofing, node capture, and side-channel attacks are detailed alongside effective countermeasures, including encryption, authentication, and secure boot processes. The paper also explores the application of machine learning algorithms, such as Random Forests and Support Vector Machines, in detecting and mitigating IoT-specific threats. Security frameworks, ranging from qualitative approaches like OCTAVE to quantitative methodologies like CVSS, are also evaluated for their relevance in assessing and managing IoT vulnerabilities. This study guides the development of robust IoT security strategies based on recent research.

Keywords— IoT, Machine learning, Attacks, Security tools, Cybersecurity, Dataset, Security Frameworks

I. Introduction

The rapid development of Internet of Things technologies has made great progress in various fields. IoT devices can be found in smartphones, electrical appliances, and smart homes.

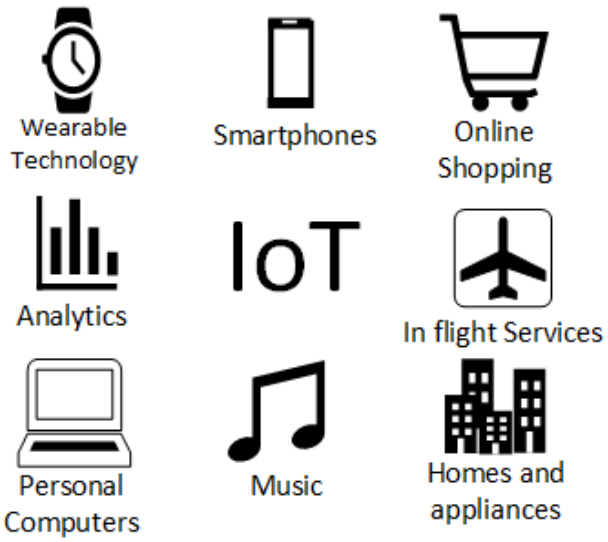

Figure 1 Internet of Things

1 Authors are with Faculty of Management Science and Informatics, University 26 Zilina, of Slovakia Zilina, Univerzitna 8215/1, 010 (corresponding author to provide phone: +421-904-039-386; e-mail: slavomir.tatarka@fri.uniza.sk), (e-mail: jozef.papan@fri.uniza.sk) 2Author is with Faculty of Electrical Engineering and Informatics, University of Pardubice, Studentsk´a 95, 532 10 Pardubice 2, Czech Republic (e-mail: jan.panus@upce.cz)

Figure 1 illustrates various IoT devices and their roles across selected domains. However, the scope of IoT extends far beyond these examples. In addition to consumer electronics and smart homes, IoT technologies are increasingly embedded in industrial automation (Industry 4.0), precision agriculture, smart transportation systems, environmental monitoring, and healthcare—ranging from wearable sensors to connected medical devices. This broad applicability underscores the growing need for robust and adaptable security mechanisms in diverse and complex environments. While they significantly enhance our daily lives, they also introduce new security challenges. As cyberattacks continue to rise, IoT security has become a frequently discussed topic in the scientific community in recent years, motivating us to explore this issue further. This paper aims to synthesise current knowledge and provide guidance for real-world applications and further research in IoT cybersecurity.

Our analysis of IoT attacks, threats, security tools, machine learning approaches, and frameworks draws upon the following key articles:

- IoT Device Attacks, Security and Certification (2024) [1]
- A Machine Learning-Based Methodology for IoT Security(2023) [2]
- A Conceptual Introduction of Machine Learning Algorithms (2023) [3]
- Preventing Spoofing Threats in IoT: Machine Learning Approaches for Intrusion Detection (2024) [4]
- Enhancing IoT Security: Machine Learning-Based Network Intrusion Detection (2023) [5]
- Securing Internet of Things Using Machine and Deep Learning Methods: A Survey (2024) [6]
- Intrusion Detection in IoT Using Deep Learning (2023) [7]
- IoT Attack Detection Method Based on Synthetic Minority Over-Sampling with Random Forest Technique (2023) [8]
- AI Security and Cyber Risk in IoT Systems (2024) [9]
- Unifying_RNN_and_KNN_for_Enhancing_Mirai_Attack_Detection_in_IoT_Networks(2024) [10]

The structure of our article is as follows: Section II focuses on the types of attacks targeting IoT devices, detailing how these attacks operate. It also analyses cybersecurity tools, explaining their purpose and applications. Section III is dedicated to machine learning, describing its various approaches and how they can be applied to enhance IoT security. Section IV discusses different security frameworks used to evaluate threats and vulnerabilities in the IoT domain. Finally, the Discussion and Conclusion sections summarise the key findings and insights presented in the article.

II. IoT SECURITY: DEVICE-LEVEL ATTACKS AND SECURITY ANALYSIS TOOLS

This section describes often-occurring attacks on Iot infrastructure and possible defence mechanisms.

A. *Device-level attacks*

The following section is based on information from [1].

- Device Spoofing: Device (IoT) spoofing is a technique in which an attacker impersonates a legitimate device within the network they intend to attack, using it to gain unauthorised access. The attacker can initiate an attack from within the system through this manipulation. Protection against such attacks includes methods such as localisation (determining the device's position), detection based on transmission channel analysis, or authentication.
- Device Cloning: Device cloning occurs when an unauthorised individual duplicates a device's identity onto another. The primary goal of this attack is typically identity theft. Attackers employ various methods for this attack, focusing mainly on mobile device SIM cards and unique identifiers. Protective measures against such attacks include symmetric encryption, public key-based solutions using random numbers, and fingerprint communication. These measures help distinguish the legitimate device from the cloned one.
- Non-repudiation ensures that the origin of data can be definitively verified, preventing the sender or recipient from denying their involvement. While it is not universally mandatory in all IT contexts, maintaining accountability in certain IoT applications—such as healthcare and transportation—is critical. Malicious actors can forge transactions or overload the system if non-repudiation is compromised, potentially leading to denial-of-service (DoS) attacks.
- Node Capture Attack: In this type of attack, an attacker takes control of an IoT node, such as a sensor, allowing them to obtain or modify data on that node. Attacks on nodes can lead to the leakage of sensitive information and subsequent security compromises. This attack can be prevented by using data encryption, authentication, software updates and especially physical security.
- Side-Channel Attack, SCA: An attack that analyses indirect physical effects during system operation to obtain sensitive data. Attackers monitor, for example, electromagnetic radiation, energy consumption, operation timing, or acoustic signals. These methods allow the attacker to extract secret data, such as cryptographic keys, and compromise the security of the IoT system. Modern devices are already mostly made to be resistant to this attack. However, suppose a device is not secured against this type of attack. In that case, it is difficult to detect it subsequently because it does not leave direct traces or interfere with the system's normal operation. Physical shielding, noise injection, or the best secure hardware modules can be used to protect against this attack.
- Eavesdropping and Interference: Since IoT devices are often placed in open areas, they are vulnerable to eavesdropping, which can lead to data leakage during transmission. Interference can cause devices to stop working properly or the connection to be interrupted, increasing the system's vulnerability. The best protection against this attack is data encryption.
- Sleep Deprivation Attacks: In this attack, the attacker aims to drain the device's battery. Battery depletion makes the system vulnerable to a Denial of Service attack. The attacker can increase the device's power consumption by manipulating its processes, such as injecting infinite cycles or other methods that cause excessive load, which causes the device to wear out faster. This shortens the device's lifespan, which can lead to downtime or failure. Such attacks can seriously affect devices in areas such as healthcare or security, where continuous functionality is crucial. To protect against this attack, a device should be able to monitor its power consumption. Knowing about power consumption allows the device to detect behavioural anomalies that indicate an attack has occurred.
- Booting Attacks: These are attacks that allow an attacker to compromise a device during the boot process when security measures are not yet in place. They are difficult to detect due to IoT devices' sleep and wake cycles. Protective measures include secure boot, firmware encryption, or ensuring that the attacker does not have physical access to the device.

Table 1 Attacks and defenses

Attack type	Description	Defense
Device spoofing	Impersonation of a legitimate device to gain access	Authentication, localization, channel analysis
Device Cloning	Copying a device’s identity for unauthorized use	Symmetric/public-key encryption, fingerprint communication
Node Capture	Physical takeover of a sensor or node	Physical security, encryption
Side-Channel Attack	Analysis of physical emissions	Shielding, noise injection, secure hardware modules
Eavesdropping	Listening or disrupting wireless communication	Strong encryption, interference resistance
Sleep Deprivation	Draining the battery by keeping the device active	Power monitoring, behavioral anomaly detection

Booting Attack	Attack during startup before full security is active	Secure boot, firmware encryption, restrict physical access

B. Cybersecurity analysis tools

The following analysis of cybersecurity tools is derived from [1].

1. Wireshark: Wireshark analyses network protocols. It captures and inspects network traffic to detect non-standard or suspicious packets. By closely monitoring communication patterns between IoT devices and the network, Wireshark helps identify vulnerabilities and threats in an IoT environment.
2. Nmap scans networks to identify active devices and their open ports (TCP/UDP). It can also perform OS detection, version detection, and discover services like Telnet or SSH (typically running on ports 23 and 22). This functionality helps reveal potential vulnerabilities and misconfigurations. Nmap can also verify firewall settings or identify outdated and unsafe services in an IoT network.
3. Binwalk: Binwalk is a binary analysis tool that uses the libmagic library. It enables the extraction of firmware images to access the operating system or applications used in IoT devices. This approach can help uncover malware, misconfigurations, and vulnerabilities in firmware.
4. Burp Suite: Burp Suite tests the security of IoT web interfaces. It includes several modes: proxy (to intercept and modify HTTPS requests), intruder (to test resistance to attacks like SQL injection or XSS), and scanner (to detect vulnerabilities, available in the paid version automatically). In the context of IoT, it can help secure web interfaces for smart devices.
5. Flawfinder: Flawfinder identifies potential security issues in source code written in C and C++. It looks for risky functions, improper memory handling, or other flaws that could lead to buffer overflow attacks or unauthorised memory reads, which can compromise an IoT device.
6. Masscan is similar to Nmap but specialises in fast scans of open TCP ports. It does not scan UDP ports nor provide as much detail about discovered devices. However, it is ideal for large-scale networks with hundreds or thousands of devices, where quickly identifying basic information is a priority.
7. Postman: Postman is used for API testing. It simulates requests, analyses server responses, and tests different communication scenarios between applications. In IoT, Postman is often employed to verify the functionality and security of smart devices, such as a thermostat sending data to a cloud server. It can determine whether the API is working correctly, whether communication is encrypted, and whether the connection is protected from unauthorised access or data leaks.
8. Cryptography Libraries: At the gateway layer, cryptographic libraries such as OpenSSL, mbedTLS, and WolfSSL are crucial for establishing secure channels (e.g., TLS/SSL) between IoT devices and the gateway. Encrypting data in transit safeguards sensitive information against eavesdropping, man-in-the-middle attacks, and other threats. This level of protection helps maintain data integrity and ensures compliance with security requirements in IoT environments.

Table 2 Cybersecurity Analysis Tools

Layer	Tool
Device layer	Flawfinder
Network layer	Nmap, Masscan, Wireshark
Gateway layer	Binwalk, Cryptography libraries
Application layer	Burp Suite, Postman.

Cybersecurity analysis tools are divided according to the layers of the IoT architecture in Table 2.

III. Machine learning in IoT

Machine learning (ML) offers another approach to enhancing the security of IoT devices, particularly for detecting and mitigating internet-based threats.

Machine learning (ML) is a branch of artificial intelligence that develops algorithms enabling systems to learn from data without explicit reprogramming. By identifying and modelling patterns, ML techniques can make predictions or classify data more accurately over time.

A dataset typically contains real-world observations from network traffic and IoT devices (e.g., sensors or smart appliances). It serves as the foundation for training ML algorithms. For instance, a dataset may include device metrics recorded during a DoS attack, enabling an ML model to recognise signs of an attack in the future. [4][5]

A. Types of machine learning

The following types, discussed in [2] and [3], are particularly relevant for IoT security:

1) Supervised learning

Algorithms receive labelled datasets, where each input is paired with a known target output. Models learn these input-output relationships and apply them to new, unseen data. Supervised learning effectively detects IoT attacks (e.g., DoS, spoofing, malware) and predicts device failures. Common algorithms include Support Vector Machines (SVM), Naive Bayes, K-Nearest Neighbors (KNN), neural networks, deep neural networks (DNN), and Random Forests.

2) Unsupervised learning

Here, algorithms operate on unlabeled data to detect inherent structures or clusters. This is particularly useful for anomaly detection in network traffic, including DoS and DDoS attacks. By grouping unusual patterns, unsupervised methods can flag suspicious activity in IoT environments.

3) Reinforcement learning (RL)

Reinforcement Learning (RL) is a type of machine learning where an agent—such as an IoT device—learns optimal behavior by interacting with its environment. Actions that result in positive outcomes are rewarded, while negative outcomes incur penalties. This iterative learning approach enables IoT devices to dynamically adapt their security strategies in response to evolving threats such as denial-of-service (DoS), spoofing, or malware. Common RL algorithms applied in this context include Q-learning, Dyna-Q, Post-Decision State (PDS), and Deep Q-Networks (DQN).

These categories do not encompass every ML method available, but they highlight those most commonly applied to IoT scenarios in the referenced literature.

B. Machine learning methods

1) Support Vector Machines (SVM)

Support Vector Machines (Fig. 2) are widely used for classification and regression tasks. They identify a hyperplane (or multiple hyperplanes) that maximises the margin between different classes, thereby enhancing classification accuracy. As illustrated in Figure 2, each colour cluster (red, blue, green) is separated by a boundary. In IoT security, an SVM can be trained on datasets containing normal user behaviour and known attack patterns—such as spoofing or malware—to distinguish legitimate from illegitimate traffic effectively.

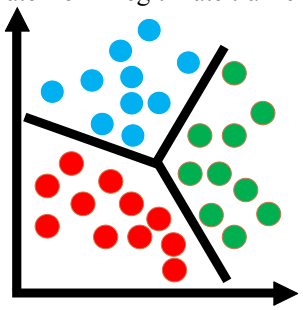

Figure 2 SVM

2) Naive Bayes (NB)

Naive Bayes (Fig. 3) is a simple yet effective classification method based on Bayes' theorem. It assumes independence among predictors—a simplification that is not always accurate but often yields strong performance. As illustrated in Figure 3, each colour cluster (blue, orange, red) can be separated by probability-based decision boundaries. Although these boundaries may appear simplified, Naive Bayes is widely used in various applications, including IoT security scenarios. For instance, it can be employed to analyse textual logs from IoT devices or gateways to detect abnormal or malicious messages. In [11], Naive Bayes helped accurately identify phishing attacks by learning the features distinguishing fraudulent emails from legitimate ones. This principle can similarly be applied to detect suspicious IoT-related communications.

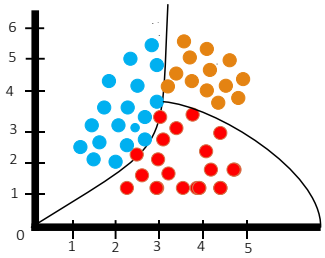

Figure 3 Naive Bayes

3) K-Nearest Neighbors (KNN)

K-Nearest Neighbors (Fig. 4) classifies data points based on the classes of their closest neighbours in a feature space. The figure shows that the system has limited knowledge about the query datapoint's class before training. Still, after training on labelled examples, the data point can be assigned to the class with the greatest similarity (in this illustration, the "positive reviews" group).

In an IoT security context, KNN proved effective for detecting Mirai attacks [10]. Mirai scans networks for IoT devices with weak credentials; once infected, they become part of a botnet that launches DDoS attacks. KNN can spot deviations from normal device behaviour—such as unusually high outbound traffic—by comparing them to known malicious or legitimate patterns. If most of the nearest neighbours exhibit attack-like traits, KNN flags the device as compromised.

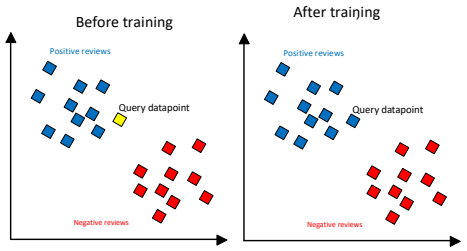

Figure 4 K-Nearest Neighbors (KNN)

4) Random Forests (RF)

Random Forests (Fig. 5) is a machine-learning method that combines multiple decision trees to improve accuracy and reduce overfitting. The figure shows that each tree is trained on a different subset of features or samples. The final prediction is determined by aggregating the outputs (e.g., majority voting) from all the individual trees. In [8], researchers applied Random Forests to IoT traffic data, where actual attack samples were relatively scarce compared to normal data. They incorporated the SMOTE (Synthetic Minority Over-sampling Technique) to address this class imbalance. SMOTE generates synthetic samples of the minority class (in this case, attack-related data) by interpolating between existing data points, thereby improving model performance on rare events. This approach boosted the accuracy of Random Forests by up to 15%, demonstrating that combining SMOTE with Random Forests can effectively detect and prevent attacks in IoT networks.

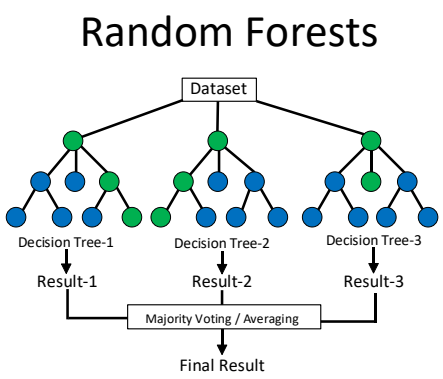

Figure 5 Random Forests

IV. Security Frameworks for IoT

IoT devices often face diverse cybersecurity challenges. To address these challenges, researchers and practitioners rely on various frameworks to assess the magnitude of potential risks to both systems and devices. According to [9], these frameworks differ primarily in their approach—some rely on qualitative judgments based on expert analysis, while others emphasise more quantitative methods grounded in metrics or simulations.

Below is an overview of several key security frameworks drawn from [9], highlighting their applicability and limitations in an IoT context:

1) OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a qualitative framework employing questionnaires to identify and categorise problem areas. It offers in-depth threat analysis to help organisations understand cyber risks in their environments. However, its detailed, time-intensive process may be challenging for fast-evolving IoT deployments.
2) TARA (Threat Analysis and Risk Assessment) is a predictive qualitative framework that prioritises critical vulnerabilities over a comprehensive enumeration of all potential risks. Its chief advantage is efficient resource allocation, which is the first to mitigate the most damaging threats. However, TARA requires thorough domain knowledge to correctly identify key vulnerabilities, which can be difficult in complex IoT ecosystems.
3) CVSS (Common Vulnerability Scoring System) employs both numeric scores (ranging from 0 to 10) and descriptive ratings (e.g., "Low," "Medium," "High," and "Critical") to evaluate the severity of vulnerabilities. It is widely used to benchmark software flaws, making it useful for IoT devices with common protocols or operating systems. Although partially quantitative, CVSS results often need additional context to translate severity scores into actionable risk decisions.
4) Exostar System: Exostar is primarily a qualitative framework tailored to multi-tier partnerships and supply chains. It identifies regulatory and security gaps in extended business networks. While supply chain security is relevant to IoT (especially where multiple vendors provide device components or services), Exostar's approach may be too specialised for purely device-level risk analysis.
5) CMMI (Capability Maturity Model Integration) integrates best practices from systems analysis, software engineering, and project management. It aims to improve overall organizational security and process maturity. Though powerful, CMMI can be cumbersome and requires significant expertise—a potential drawback for agile IoT environments where rapid deployment is common.
6) The NIST Cybersecurity Framework provides a comprehensive, policy-level structure to identify, protect, detect, respond to, and recover from cyber incidents. Despite broad acceptance across industries, it was not specifically designed for IoT. Adapting it to IoT devices' varied protocols and resource constraints may require specialised guidelines or extensions.
7) CyVaR (Cyber Value at Risk) is a quantitative framework that applies Monte Carlo simulations to evaluate cybersecurity risks. Modelling probabilities and potential financial impacts can yield more precise damage estimates. However, modelling heterogeneous IoT devices with unique protocols and threat profiles can complicate the simulation process.

V. Discussion

This section synthesises key insights from the preceding chapters, highlighting interdependencies and suggesting future considerations.

A. IoT Attacks and Defenses

Device-level threats remain prevalent due to limited resources, diverse protocols, and poor update practices. Attacks—ranging from spoofing to boot-time exploits—require mitigation tailored to each device's role and capabilities.

- Physical-based attacks (Side-Channel, Node Capture) benefit most from physical shielding, strong authentication, and regular firmware updates.
- Network-based attacks (Eavesdropping, Spoofing, Sleep Deprivation) often require strong encryption, real-time intrusion detection, and traffic analysis tools.
- Boot-level vulnerabilities highlight the need for secure boot processes, firmware encryption, and restricting physical device access.

B. Cybersecurity Tools for IoT

Section II-B reviewed tools such as Wireshark, Nmap, Binwalk, Burp Suite, Flawfinder, Masscan, Postman, and cryptographic libraries for analysing and mitigating IoT threats. These are typically deployed by layer: Flawfinder and Binwalk target device-level issues, Nmap and Wireshark focus on network layers, while Postman and Burp Suite secure application interfaces. Masscan is suited for large-scale network scans. A key challenge remains their integration across diverse, proprietary IoT environments.

C. Machine Learning for Improved Detection

Section III highlighted the potential of supervised learning to detect anomalies in large, heterogeneous IoT data streams.

Methods like Random Forests, Naive Bayes, and SVMs are effective, though often require techniques such as SMOTE to address class imbalance. While deep networks offer high accuracy, interpretable models like decision trees or KNN remain valuable for debugging and regulatory compliance.

Despite its potential, ML requires robust feature engineering, regular model updates, and integration with additional security mechanisms.

D. Security Frameworks for Tailored Risk Assessment

In Section IV, we compared frameworks (e.g., OCTAVE, TARA, CVSS, Exostar, CMMI, NIST, CyVaR) and found that each serves a different organisational context:

- Qualitative approaches (OCTAVE, TARA, Exostar, CMMI, NIST) allow rapid classification of IoT threats but can be subjective.
- Quantitative methods (CyVaR) can yield more precise outcomes but demand robust modelling capabilities—a challenge when IoT systems involve diverse devices lacking standardised security metrics.
- Hybrid approaches (CVSS) provide numeric severity scores and textual labels, bridging technical detail with high-level risk communication.

Framework choice should reflect project scale, data availability, domain regulations, and organisational resources.

E. Practical Considerations and Future Perspectives

Several practical factors influence the real-world deployment of IoT security. ML methods such as Random Forests, SVM, KNN, and Naive Bayes show strong intrusion detection performance, though results depend on data quality, model complexity, and device constraints. Lightweight models suit low-power devices, while complex ones perform better in cloud environments. Frameworks like CVSS, OCTAVE, and CyVaR support risk evaluation through structured, context-aware assessment. Effective strategies combine proactive threat modelling, anomaly detection, and layered defense, as demonstrated by real-world attacks such as Mirai.

VI. Conclusion

This article provided a structured overview of current IoT security threats, countermeasures, machine learning-based detection techniques, and risk assessment frameworks. The layered analysis—from device-level attacks to architectural defense mechanisms—highlights the multifaceted nature of IoT cybersecurity. By synthesising recent literature and practical approaches, this study offers a valuable reference point for researchers and practitioners seeking to design scalable, resilient, and resource-aware security strategies for heterogeneous IoT environments. Comparing frameworks further supports decision-making for risk management across varying deployment scenarios.

Acknowledgement

This paper is supported by project KEGA 004 ˇZU-4/2024 ”Improving the quality of education in the field of cyber security”.

Funded by the European Union NextGenerationEU through the Recovery and Resilience Plan for Slovakia under the project No.17R05-04-V01-00005.

References

[1] S. Keshary, K. Venkatesan, T. Padmapritha, S. Srinivasan, and S. Seshadhri, “IoT Device Attacks, Security and Certification,” *Proc. Int. Conf. Circuit Power Comput. Technol. ICCPCT 2024*, pp. 36–42, 2024, doi: 10.1109/ICCPCT61902.2024.10672639.

[2] “A Machine Learning-Based Methodology for IoT Security | IEEE Conference Publication | IEEE Xplore.” https://ieeexplore.ieee.org/document/10200330 (accessed Nov. 26, 2024).

[3] M. Kumar, S. Ali Khan, A. Bhatia, V. Sharma, and P. Jain, “A Conceptual Introduction of Machine Learning Algorithms,” *2023 1st Int. Conf. Intell. Comput. Res. Trends, ICRT 2023*, 2023, doi: 10.1109/ICRT57042.2023.10146676.

[4] “Preventing Spoofing Threats in IoT: Machine Learning Approaches for Intrusion Detection | IEEE Conference Publication | IEEE Xplore.” https://ieeexplore.ieee.org/document/10730888 (accessed Nov. 27, 2024).

[5] “Enhancing IoT Security: Machine Learning-Based Network Intrusion Detection | IEEE Conference Publication | IEEE Xplore.” https://ieeexplore.ieee.org/document/10269850 (accessed Nov. 27, 2024).

[6] A. Ghaffari, N. Jelodari, S. pouralish, N. derakhshanfard, and B. Arasteh, “Securing internet of things using machine and deep learning methods: a survey,” *Cluster Comput.*, vol. 27, no. 7, pp. 9065–9089, Oct. 2024, doi: 10.1007/S10586-024-04509-0/FIGURES/6.

[7] A. M. Banaamah and I. Ahmad, “Intrusion Detection in IoT Using Deep Learning,” *Sensors 2022, Vol. 22, Page 8417*, vol. 22, no. 21, p. 8417, Nov. 2022, doi: 10.3390/S22218417.

[8] “IoT Attack Detection Method based on Synthetic Minority Over-Sampling with Random Forest Technique | IEEE Conference Publication | IEEE Xplore.” https://ieeexplore.ieee.org/abstract/document/10112425 (accessed Nov. 30, 2024).

[9] P. Radanliev, D. De Roure, C. Maple, J. Nurse, R. Nicolescu, and U. D. Ani, “AI Security and Cyber Risk in IoT Systems,” *Front. Big Data*, vol. 7, p. 1402745, doi: 10.3389/FDATA.2024.1402745.

[10] A. Kumari, D. Gupta, and M. Uppal, “Unifying RNN and KNN for Enhancing Mirai Attack Detection in IoT Networks,” *2024 IEEE Int. Conf. Inf. Technol. Electron. Intell. Commun. Syst. ICITEICS 2024*, 2024, doi: 10.1109/ICITEICS61368.2024.10625616.

[11] A. M. Banaamah and I. Ahmad, “Intrusion Detection in IoT Using Deep Learning,” *Sensors*, vol. 22, no. 21, 2022, doi: 10.3390/s22218417.