Grenze International Journal of Engineering and Technology, June Issue

Machine Learning based IoT Security: A Systematic Review

Fatma Said Sleyum[1], Aparna Sharma[2] and Mansi Fartyal[3]
[1-3]Department of Computer Science & Applications Sharda School of Computing Sciences & Engineering Sharda University, Greater Noida, India
Email: 2024876215.fatma@ug.sharda.ac.in, aparnaa.mca@gmail.com, 2024503138.mansi@ug.sharda.ac.in

***Abstract*— IoT is growing very fast and is used in different sectors like healthcare, transportation, education, agriculture, and smart homes by connecting different devices through net-works. IoT uses internet connectivity than traditional devices like desktops and laptops. Due to this growth, IoT faced security challenges such as unauthorized access and other malware at-tacks. Machine Learning techniques are used to detect anomalies, identify unusual behaviors, and prevent attacks. Our research focuses on how Machine learning can be used to prevent attacks and protect IoT devices, ensuring that they are fully secured. Furthermore, our study shows the common vulnerabilities that happen in IoT devices, and how to overcome them using Machine Learning.**

***Index Terms*— Internet of Things (IoT), Machine Learning (ML), IoT security, Cybersecurity.**

I. INTRODUCTION

IoT is a growing technology that changes the way we live. As the number of combined devices increases, it's important to extend devices and networks.

IoT networks are made up of different devices attached with electronic software, sensors, and connectivity that monitor and control the world. The benefit of extending devices is to collect and analyze more data that can be used to improve overall efficiency [1].

IoT devices transmit data over the Internet in an open environment with less security capabilities since designers did not consider security capabilities since designers did not consider security while designing IoT devices. The expansion of IoT devices and communication channels attracts hackers to target different companies [2]. Common threats hackers use to attack are unauthorized access, Denial of Service (DoS), phishing, data manipulation, and malware infections.

To overcome these challenges, Machine Learning is used to ensure security in IoT devices. Machine Learning makes systems to automatically identify patterns and anomalies. This allows companies to identify new threats before they cause harm [3].

Our research focuses on analyzing how machine learning protects IoT systems and prevents all types of attacks to make sure they are fully secured.

The study also involves all possible attacks that occur in IoT environments, the challenges of using Machine Learning Techniques for security, and steps to secure IoT infrastructure [4].

Grenze ID: 01.GIJET.12.2.75_20
© Grenze Scientific Society, 2026

II. BACKGROUND

A. Introduction to IoT

IoT stands for Internet of Things. It can be defined as the network of combined objects that are attached with identifiers that enable them to get data and exchange it without any interaction. IoT started in 1982 as a vending machine; its function was to report if the drinks were cold and available. During the 1990s first IoT prototype was created by John Romkey by creating a toaster that could be turned on and off through the internet, then A British technologist Kevish Ashton gave the term Internet of Things while he was at Procter and Gamble [5]. In the 2000s, the IoT devices became very popular and were used by people. LG announced a smart refrigerator that can order groceries online, and Google started collecting Wi-Fi data for Street View to show how IoT is everywhere. During the 2020s to present, IoT is now part of smart cities, health care, transport, and industries, and technology and making IoT faster and more efficient [6].

IoT came into existence using 4 main components that worked together to enable connectivity and decision-making. The Components are Devices and sensors that collect data from the environment, Connectivity that transmits data be-tween devices and platforms, Data processing that processes data into meaningful information, and a User Interface (UI) where users interact with the IoT system [7].

B. IoT Architecture

IoT architecture is the backbone of an IoT system, which shows how smart devices interact to process and interchange data. It acts as the foundation of all connected devices; it ensures smooth communication and security [8]. IoT archi-tecture consists of three layers, which are the Physical Layer (Perception layer), which includes edge devices, sensors, and actuators for communication and detection. Network Layer, which distributes and stores data, links smart objects, network devices, and servers, also supports device communication and devices-to-server communication [9]. Application Layer, which is the Layer where users communicate, provides cus-tomers with software resources, and it also monitors and controls IoT devices remotely.

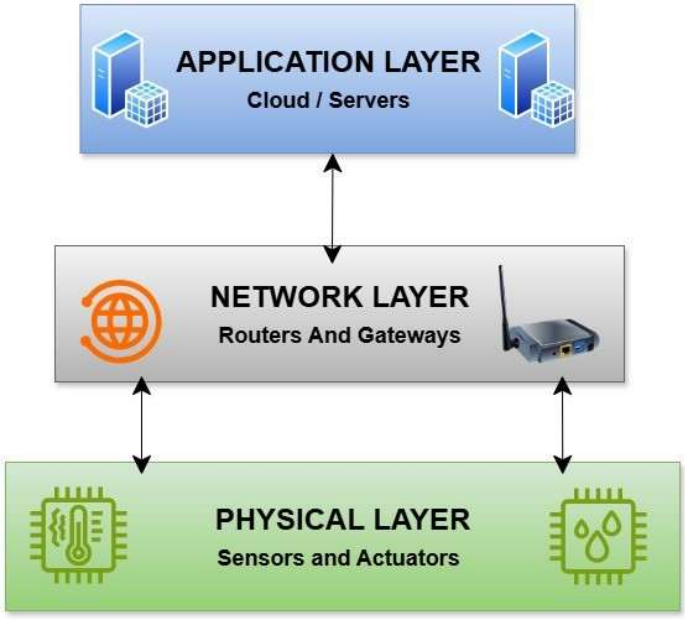

Fig. 1. Architecture of IoT

The main goals of IoT are to save time by doing simple jobs using IoT devices. Scalability, which is the addition of new devices in a system without affecting other devices that were connected before [10]. Improve safety and security by detecting attacks as early as possible and giving an alert before problems happen that will affect the whole system. Easy connectivity, by connecting multiple devices together through a network and communicating. Automation, devices work by their own without involving human help, that way life becomes smooth [11].

C. Attacks on IoT Systems

IoT devices are built to fulfill the needs of an organization; therefore, they lack security protocols. Attackers use this opportunity to attack any of the weak IoT devices [12]. They install malware on the device and harm it or gain access to other personal data of the company. The most common IoT attacks include the following:

- Physical Attacks: Hackers find the location of the device and take data from it. Attackers attack the devices physically instead of attacking them through the network like other malware [13].
- Denial of Service (DoS) and Distributed Denial of Service (DDoS): These happen when attackers use multiple computers to flood a server or website [14] with too much traffic at the same time to make it unavailable [15].
- Malware and Ransomware Attacks: Malware is software which are made to harm devices or systems. Ransomware is a malware attack whereby hackers lock files and devices, then ask for money (ransom) to unlock them [16].
- Data Breach and Privacy Attacks: These are attacks whereby an attacker hacks devices, steals identity, and accesses data of organizations or individuals without their permission [17].

In our research, we discovered that IoT devices create a smart environment, but they are easy to be attacked. This is because IoT devices are used in many places, and they do not follow strong security standards.

We can protect IoT systems and devices by using security techniques, including encryption, authentication to identify harmful activities [18].

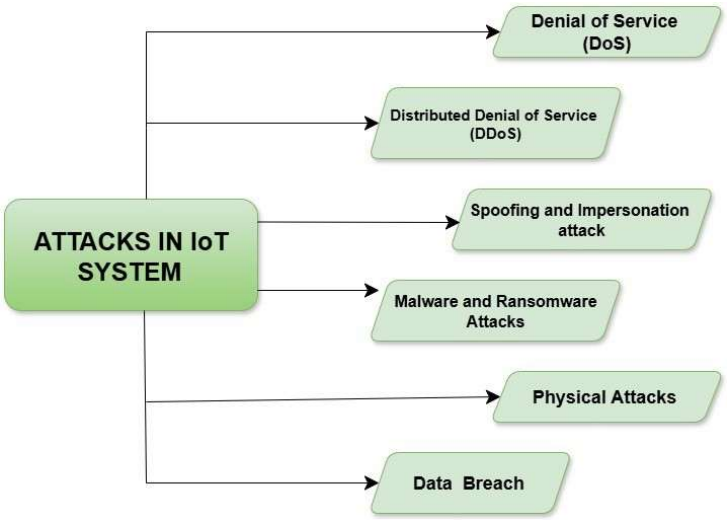

Fig. 2. Layer-wise attacks in IoT Communication

III. LITERATURE REVIEW

The increase in IoT devices has caused security challenges, making intrusion detection and threat prevention systems a critical part of research. Machine Learning (ML) and Deep learning (DL) act as powerful tools to solve these challenges. This review shows the recent literature on ML-based security solutions for IoT networks. A primary focus of recent research has developed ML that operates in a resource-constrained and dynamic environment of IoT. Several studies showed remarkable success in this area [19]. For instance, A model achieved 99.9% accuracy in detecting different types of attacks than existing methods. Also, Cross-layer features with the Cat Boost Algorithm provided the efficiency of IDS/IPS in real-time detection and prevention. Different algorithms show that

Gradient Boosting performed 89.34% accurately than Random Forest and Decision Trees (~ 82%) and better than SVM (54.72%).

However, using Machine Learning in IoT security also has many challenges; a big problem is data. There are not enough datasets, labelling data is costly, and datasets are imbalanced. There are a few benchmark datasets. In the future, researchers suggest different directions; there is a need to build lightweight Machine Learning models that run on IoT and edge devices. Also, Blockchain and federated learning are recommended [20].

In Conclusion, through this research, we found that Machine learning can improve IoT security, but future work must reduce data problems, make models faster and more transparent to secure IoT systems.

IV. Machine Learning Techniques to Secure Communication in IoT

Machine learning (ML) has become an essential tool in enhancing security in IOT devices due to different challenges faced by IoT networks. An IoT network consists of several devices with different resource capabilities and communication protocols, which makes traditional security often insufficient [21]. Machine Learning secures communication in these en-vironments by detecting anomalies, preventing attacks, and improving authentication and encryption techniques. The com-mon Machine Learning Techniques used to secure communi-cation in IoT systems include the following:

A. Anomaly Detection

It's a common Machine Learning Technique used to secure IoT networks. It trains models to recognize normal behaviours of IoT devices and their communication patterns. If the model detects unusual behaviour, it flags it as a potential threat [22].

B. Intrusion Detection Systems (IDS)

This system is designed for detecting unauthorized access in IoT networks. It uses decision trees, Naive Bayes classifiers, and Neural Networks to protect IoT devices such as cameras, sensors, or smart home appliances from attacks by identifying traffic patterns [23].

C. Traffic Analysis and Flow Monitoring

Machine learning is also used to monitor IoT network traffic and identify patterns that may indicate attacks. Machine Learning models can detect threats that traditional mechanisms cannot. It uses a Clustering algorithm and Reinforcement learning to detect unauthorized devices that indicate botnet-based attacks [24].

D. Malware Detection

Most IoT devices are vulnerable to malware attacks that can steal sensitive information. Machine Learning can be used to detect malware signatures that occur in IoT device communications. It uses signature-based detection, Behaviour-based detection, and deep learning to detect IoT devices that are infected by Ransomware or botnet malware that send data to external command and control servers [25].

Table I: Summary of Reviewed Literature

Year	Authors	Key Findings	Limitations
2024	Abdullah Alomini, Shailendra Mishra, Mohammed alshehri	Machine Learning based security that detect and prevent cyberattacks that happen in IoT networks	It faced Limited data, fixed features, class im-balance and scalability issues
2022	Ghulam Abbas, Amjad Mahmood, Jaime Lloret, et al.	Safety, security and privacy in Machine Learning based IoT	It faced issues concerning data security and privacy issues, weak backups, high ML cost, and infrastructure vulnerabilities
2023	Abdulrahman K, Alnaim and Ahmed M Alwakeel	Machine Learning based IoT in edge Computing in Healthcare	Managing massive IoT data, ensuring privacy and security and handling computational bottlenecks
2021	Tanzila Saba, Khalid Haseeb, Asghar Ali Shah, et al.	Machine Learning- Based Intrusion Detection for autonomous security in IoT	Traditional routing methods struggle with dynamic network conditions that affect reliability and security
2025	Noor Hafsa, Hadeel Alzoubi and Sajda Imran	Machine Learning based intrusion detection and prevention by using Cross-layer Features in IoT networks	Limited attack labels and dynamic network conditions that affect reliability and security
2025	Zhe Deng	Machine Learning based intrusion detection for IoT environments	High cost of labeling, presence of threats, data scarcity and heterogeneous devices

E. Encryption and Authentication

Machine Learning techniques can be used for Encryption and Authentication mechanisms used in IoT systems. It uses adaptive key generation, behavioral Authentication, and Deep learning for Cryptography to ensure that only authorized devices get access to the IoT network, hence it reduces the number of attacks associated with stolen or guessed credentials [26].

Machine Learning Techniques are useful in securing communication in IoT networks. Through our research, we dis- covered the use of anomaly detection, intrusion detection, traffic analysis, malware detection, and advanced

encryption and Authentication methods as essential Machine Learning Techniques that can enhance defences against various cyberat-tacks. As days go on, Machine Learning will keep on growing to secure many connected devices in the IoT ecosystem [27].

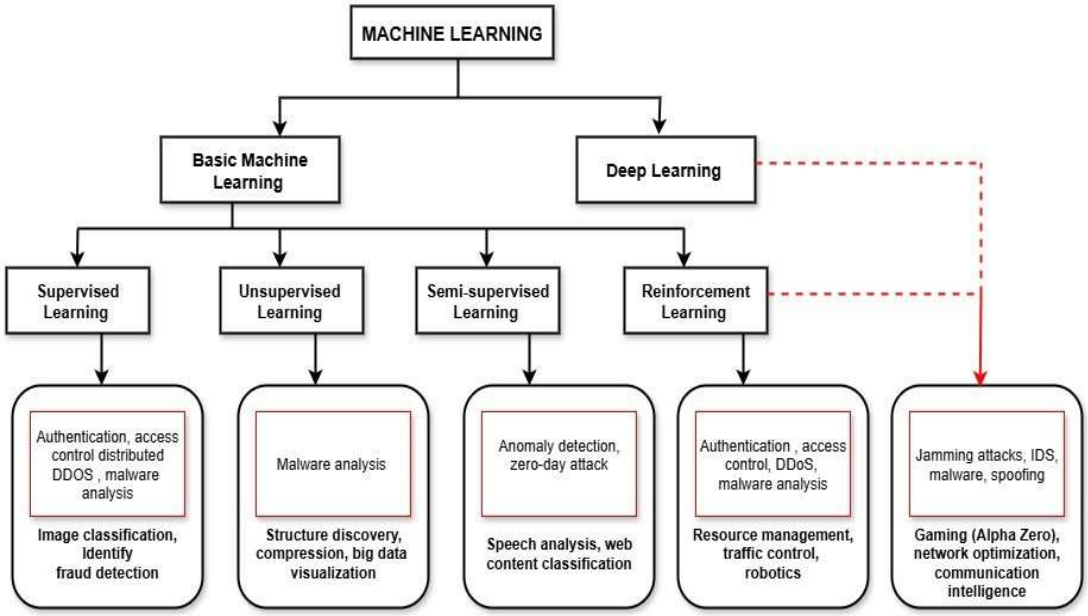

Fig. 3. Machine learning classes and applications

F. Machine Learning Techniques to Detect Attacks in IoT Systems

Machine learning is very important in improving security in IoT systems. It can learn patterns, detect unusual behaviours, and detect attacks faster than traditional methods. It can also automatically study network traffic, sensor readings, and recognize threats such as malware, DDoS, and unauthorized access. Machine Learning Techniques used to detect attacks in IoT ecosystems are as follows:

- Supervised Learning: It's a machine learning technique that uses labelled data for training. It classifies traffic as either normal or attacks based on historical data. It contains:
  - Decision trees: They create a series of decision rules based on input features.
  - Support Vector Machines: It's used for classification processes. It finds the best boundary, called a Hyperplane, that separates different classes in data [28].
  - Random Forest: It uses decision trees to make predic-tions. This helps improve the accuracy and reduce errors.
- Unsupervised Learning: It's a machine learning tech-nique in which labelled data is not available.
  - K-means Clustering: It groups data and organizes them based on their similarities.
  - DBSCAN (Density Based Spatial Clustering of Appli-cations with Noise): It groups data based on their density and identifies the dense regions in the data space as the clusters.
  - Isolation Forest: It isolates data points that are sig-nificantly different from the normal observations using random partitioning [29]. It enables quick identification with low computational effort.
- Deep Learning: It's the way in which machines under-stand, learn, and interact with complex data. It makes com-puters uncover patterns and make decisions from unstructured data. Convolutional Neural Networks (CNNs) are used to process data from grid-like matrix datasets.
- Ensemble Learning: It's a method where we combine many models to get a better and more accurate answer. It can be in three ways: Bagging, where models are trained independently in different subsets, boosting, where models are trained one by one, and stacking, which involves multiple different models and is used as input to find a final model [30].
- Reinforcement Learning: It's a machine learning in which machines learn through feedback, trials, and errors to maximize competitive rewards. This feedback comes in the form of rewards or penalties.

TABLE II: MACHINE LEARNING TECHNIQUES

Technique	Models/ Algorithms	Application
Supervised Learning	Decision trees, SVM, Random Forest	Classify network traffics, detect known at-tack patterns
Unsupervised Learning	K-means, DBSCAN, PCA	Identify anomalies and unknown attacks with-out labeled data
Semi Supervised Learning	Self-Training, Label propagation, Co-training	Uses limited labeled data with large amounts of unlabeled data
Deep Learning	CNNs, RNNs, LSTM, Autoencoders	Detect complex patterns and sequence analysis
Ensemble Learning	Q learning, DQN	Adaptive intrusion detection and resource management
Reinforcement Learning	Bagging, Boosting, Stacking	Improve accuracy of detection by combining classifiers

V. CONCLUSION

The use of machine learning in IoT security helped on how to secure the IoT devices against different threats, such as DoS, unauthorized access, and malware attacks, through different technologies. These methods enable computers to learn from data and improve performance.

However, some IoT security threats can't be solved using Machine Learning Techniques, such as physical attacks on sensors, default passwords, advanced attacks like Advanced Persistent Threats (APTs), which are due to challenges in data availability and computational resources.

In the future, this field can grow when we solve current problems, such as using lightweight models, privacy models, and Explainable AI (XAI) to secure IoT systems.

REFERENCES

[1] A. Alrefaei and M. Ilyas, "Using Machine Learning Multiclass Classi-fication Technique to Detect IoT Attacks in Real Time," Sensors, vol. 24, no. 14, p. 4516, 2024.

[2] Md. A. Hossain et al., "Deep learning-based intrusion detection for IoT networks: a scalable and efficient approach," EURASIP Journal on Information Security, Article 28, 2025.

[3] Y. Ahmed, K. Beyioku, and M. Yousefi, "Securing smart cities through machine learning: A honeypot-driven approach to attack detection in Internet of Things ecosystems," IET Smart Cities, vol. 6, no. 3, pp. 180-198, 2024.

[4] "Machine Learning-Based Security Solutions for IoT Networks: A Comprehensive Survey," Sensors, vol. 25, no. 11, p. 3341, 2025.

[5] M. Almohaimeed, R. Alyoubi, A. Aljohani, and F. Albalwy, "Use of Machine Learning and Deep Learning in Intrusion Detection for IoT," Advances in Internet of Things, vol. 15, no. 2, pp. 17-32, 2025.

[6] A. Alrefaei and M. Ilyas, "Using Machine Learning Multiclass Classi-fication Technique to Detect IoT Attacks in Real Time," Sensors, vol. 24, no. 14, p. 4516, 2024.

[7] P. Asghari, A. M. Rahmani, and H. H. S. Javadi, "Internet of Things applications: A systematic review," Computer Networks, vol. 194, p. 108169, 2022.

[8] M. B. Limpek, M. Papaioannou, G. Choudhary, and N. Dragoni, "Advancements in Machine Learning-Based Intrusion Detection in IoT: Research Trends and Challenges," Algorithms, vol. 18, no. 4, p. 209, 2025.

[9] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for Internet of Things (IoT) security," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1646-1685, 2020.

[10] Y. Ahmed, K. Beyioku, and M. Yousefi, "Securing Smart Cities through Machine Learning: A Honeypot-Driven Approach to Attack Detection in Internet of Things Ecosystems," IET Smart Cities, vol. 6, no. 3, pp. 180-198, 2024.

[11] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, vol. 76, pp. 146-164, 2018.

[12] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1686-1721, 2020.

[13] M. A. Hossain et al., "Deep Learning-Based Intrusion Detection for IoT Networks: A Scalable and Efficient Approach," EURASIP Journal on Information Security, Article 28, 2025.

[14] R. Jablaoui, O. Cheikhrouhou, and M. Hamdi, "Deep Learning Enabled Intrusion Detection System for IoT Security," EURASIP Journal on Wireless Communications and Networking, Article 66, 2025.

[15] "Machine Learning-Based Security Solutions for IoT Networks: A Comprehensive Survey," Sensors, vol. 25, no. 11, p. 3341, 2025.

[16] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for Internet of Things (IoT) security," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1646-1685, 2020.

[17] S. Li, L. Da Xu, and S. Zhao, "The Internet of Things: A survey," Information Systems Frontiers, vol. 22, no. 2, pp. 243-259, 2020.

[18] N. Kaur and N. Sood, “An energy-efficient architecture for the Internet of Things (IoT),” IEEE Systems Journal, vol. 15, no. 3, pp. 1-9, 2021.
[19] A. H. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: Enabling technologies, protocols, and applications,” IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, 2020.
[20] J. Heikkila¨ and P. Kim, “A historical overview of the Internet of Things: Key developments from the 1980s to the 2020s,” Journal of Network and Computer Applications, vol. 211, p. 103496, 2023.
[21] K. Ashton, “That ’Internet of Things’ Thing,” RFID Journal, 2009.
[22] M. E. Porter and J. E. Heppelmann, “How smart, connected products are transforming competition,” Harvard Business Review, vol. 92, no. 11, pp. 64-88, 2014.
[23] D. Evans, “The Internet of Things: How the Next Evolution of the Internet is Changing Everything,” Cisco Internet Business Solutions Group (IBSG), White Paper, 2011.
[24] A. M. Rahmani et al., “Smart cities and IoT: Concepts, applications, and research challenges,” IEEE Communications Magazine, vol. 55, no. 10, pp. 84-91, 2017.
[25] Y. Lu and L. Xu, “Internet of Things (IoT) Cybersecurity Research: A Review,” Future Generation Computer Systems, vol. 123, pp. 103-118, 2021.
[26] M. B. Limpek, M. Papaioannou, G. Choudhary, and N. Dragoni, “Advancements in Machine Learning-Based Intrusion Detection in IoT: Research Trends and Challenges,” Algorithms, vol. 18, no. 4, p. 209, 2025.
[27] R. Jablaoui, O. Cheikhrouhou, and M. Hamdi, “Deep Learning Enabled Intrusion Detection System for IoT Security,” EURASIP Journal on Wireless Communications and Networking, Article 66, 2025.
[28] P. Gupta and R. Kumar, “Architecture and components of Internet of Things (IoT),” International Journal of Advanced Research in Computer Science, vol. 12, no. 1, pp. 14-22, 2021.
[29] S. Madakam, R. Ramaswamy, and S. Tripathi, “Internet of Things (IoT): A literature review,” Journal of Computer and Communications, vol. 3, no. 5, pp. 164-173, 2015.
[30] M. Alam, J. Rufino, R. Ferreira, S. Rahman, and J. Sousa, “Interoperabil-ity and data exchange in Internet of Things systems,” Future Generation Computer Systems, vol. 113, pp. 510-518, 2020.