Journal of Systemics, Cybernetics and Informatics (2023) 21(2), 74-82
https://doi.org/10.54808/JSCI.21.02.74

A Brief Survey on the Internet of Things (IoT) Security

Abdulelah AL HANIF
Department of Electrical Engineering and Computer Science
Florida Atlantic University
Boca Raton, FL, USA

Mohammad ILYAS
Department of Electrical Engineering and Computer Science
Florida Atlantic University
Boca Raton, FL, USA

ABSTRACT [1]

The Internet of Things (IoT) is considered one of the world's fastest-growing technologies, and it has a tremendous impact on people's lives in many different ways. With notable improvements in the evolution and expansion of technologies, the IoT faces numerous security threats and challenges. IoT technology uses various devices and protocols, making it difficult to apply adequate security control across the whole system and vulnerable to multiple attacks. Using essential technologies such as ML helps in addressing the recent security challenges and attacks on the IoT ecosystem. This paper presents an overview of IoT security. Also, it highlights types of IoT architecture security and explores the various kinds of attacks under each IoT architectural layer. Moreover, this paper discusses the uses of Machine Learning (ML) as a solution in IoT systems.

Keywords: Internet of Things, Security Attacks, Machine learning.

1. INTRODUCTION

In the era of advanced technology, the IoT is one of the most notable technological developments that has undergone significant advancements. The IoT has changed the ability to interact with devices by allowing for portability and connectivity at unprecedented levels. The IoT concept refers to making devices able to connect to the internet with each other and share information seamlessly from anywhere and at any time, either through wired or wireless communication. IoT devices have the ability to collect and process enormous volumes of data, which can then be analyzed for more insights and improved decision-making. The IoT is utilized in different industries such as agriculture, water supply, energy and water management, autonomous vehicles, healthcare, and transportation.

The Internet of Things (IoT) has increased the number of devices in the technology market, which is evidence of the thriving IoT industry; however, the significant growth in the connectivity of these devices has brought security vulnerabilities and risks. Various IoT privacy and security challenges are associated with multiple IoT devices and networks. IoT devices are vulnerable to attacks because they have limited management security measures. Additionally, because multiple technologies and protocols are used in the IoT environment, it is challenging to implement efficient security among them. Also, IoT technologies collect sensitive data, so when successful attacks occur on these devices, it can lead to a loss of data and consequential economic impacts. Most IoT devices do not have the ability to sufficiently concentrate on the threat of a new type of attack, so they cannot identify assaults or vulnerabilities [1]. Therefore, IoT devices need to be more secure to mitigate and detect threats, and it is vital to increase security to maintain the data of IoT devices.

With the increasing threats in the IoT industry, there is a necessity to develop new methods to identify threats on system devices and networks. Machine learning (ML) techniques are a valuable solution to increase the stability of the entire IoT system. Recent research has shown that ML has significant potential for detecting malicious attacks by finding deviations in the IoT system and increasing the security of networks and devices. Moreover, it can decrease errors and increase the accuracy of IoT systems.

[1] We acknowledge the valuable help offered by the researchers in the Tecore Laboratory in the College of Engineering and Computer Science at Florida Atlantic University.

2. RELATED WORK

There are multiple surveys that have been published related to IoT security issues. This paper [2] provides an in-depth review of IoT security. The author discusses the taxonomy of security requirements. It also highlights recent security solutions, challenges, and future research directions.

This survey [3] gives a helpful overview of the present situation of IoT security. The author highlighted several security challenges in the IoT ecosystem and introduced various possible solutions to improve the safety of IoT, such as ML, artificial intelligence, and blockchain.

This study [4] provides an overview of machine learning as a promising technology that can enhance IoT security. The author discusses IoT architecture, future challenges, and multiple types of security attacks. It also reviews several studies that use ML as a solution in IoT security.

This paper [5] highlights certain aspects of the IoT, including threats to the IoT and multiple security solutions, addresses different security requirements and challenges, and examines the three layers of the IoT architecture.

The paper [6] introduces an overview of the development of the IoT. It highlights the most critical challenge and its application of the IoT. The authors also discuss the issue of IoT security from a layered view. A comparison is provided between anomaly detection methods and intrusion detection systems to enhance IoT security.

This paper [7] delivers an overview of the issue of IoT security and concentrates on the potential impacts of new technology to improve IoT security. It also emphasizes possible areas of future research and collaboration.

This study [8] provides a comprehensive review of IoT security. The author highlights some of the security problems that have not been adequately discussed in other literature reviews while identifying solutions, future challenges, and research areas.

This paper [9] provides a comprehensive overview of many aspects of IoT security, such as addressing new solutions (machine and deep learning), future challenges, and issues of the IoT system's architectural layers. It also highlights the significance of new strategies for continuing to develop research in IoT security. Table 1 presents a summary of some surveys on IoT security.

3. IoT LAYERED ARCHITECTURES WITH SECURITY ATTACKS

Several architectural layers of the IoT have been proposed and represented by various researchers. They consist of the following four architectural layers: the bottom layer is the perception layer, the next layer is network layer, the next layer is the middleware layer, and the top layer is the application layer [9]. Each layer is essential and performs unique tasks that cannot be done on other layers [10]. Each of these four layers is described in this section.

Perception Layer

The bottom layer is known as the sensor and perception layer. It is located at the lowest place in the IoT architectural model. It is responsible for gathering information about any given environment through the use of sensors and actuators [11]. A wide variety of sensors, including temperature and humidity sensors, as well as others, are used in the data collection process. Key technologies used in the perception layers include radio frequency identification (RFID), wireless sensor networks (WSNs), and other detecting and sensing systems [9].

Table 1. Summary of contribution surveys on IoT Security.

Reference	Year	Contribution
2	2019	It reviews security taxonomy and solutions, problems, and future research on IoT security.
3	2020	It discusses challenges in IoT security and emerging technologies that can help address security concerns.
4	2020	This survey discusses machine learning as a possible solution in IoT security and covers architecture, future, and security attacks.
5	2021	It covers the risk of IoT, security solutions, requirements, and architecture's three layers.
6	2021	It highlights the growth of IoT and the challenge of using IoT. It compared intrusion detection and Anomaly detection.
7	2022	It discusses the benefits of new technology in developing the issue of IoT security and provides potential research areas.
8	2022	It reviews IoT security in detail, some security issues, future challenges, and research opportunities.
9	2022	It covers emerging new solution technology: machine and deep learning, and future and architectural layer issues.

Network layer

The next level of the IoT architecture is the network layer. It plays a significant role in IoT-based systems because it is responsible for transmitting data assembled in the

perception layer by various devices and sensors [10]. It takes advantage of a wide variety of communication protocols, including WiFi, IEEE 802.15.4, LTA, GSM, IPv6, 3-5G, and others [12].

Middleware layer
The middleware layer of the IoT is located between the application layer and the network layer. Its responsibilities include the management of connected devices, the execution of intelligent activities, and the processing of data. It aims to automate data processing and save sensed data in a database [10]. It is widely regarded as a dependable support platform, and the technology behind it may be similar to that of cloud computing [9].

Application layer
The application layer is located on the top layer of the IoT architecture. It is in charge of delivering services to the system's end users. The IoT can be utilized in a wide variety of contexts, including smart meters, smart grids, smart healthcare, smart cities, smart energy, and smart homes [13].

4. IoT ATTACKS FOR EACH LAYER

The IoT infrastructure has been under increasing attack over the past several years, which has resulted in increased awareness on the part of manufacturers as well as end users when it comes to the creation and utilization of IoT devices. This section discusses the diverse types of attacks in each layer that can happen in the IoT. Figure 1 presents IoT security attacks for each architectural layer.

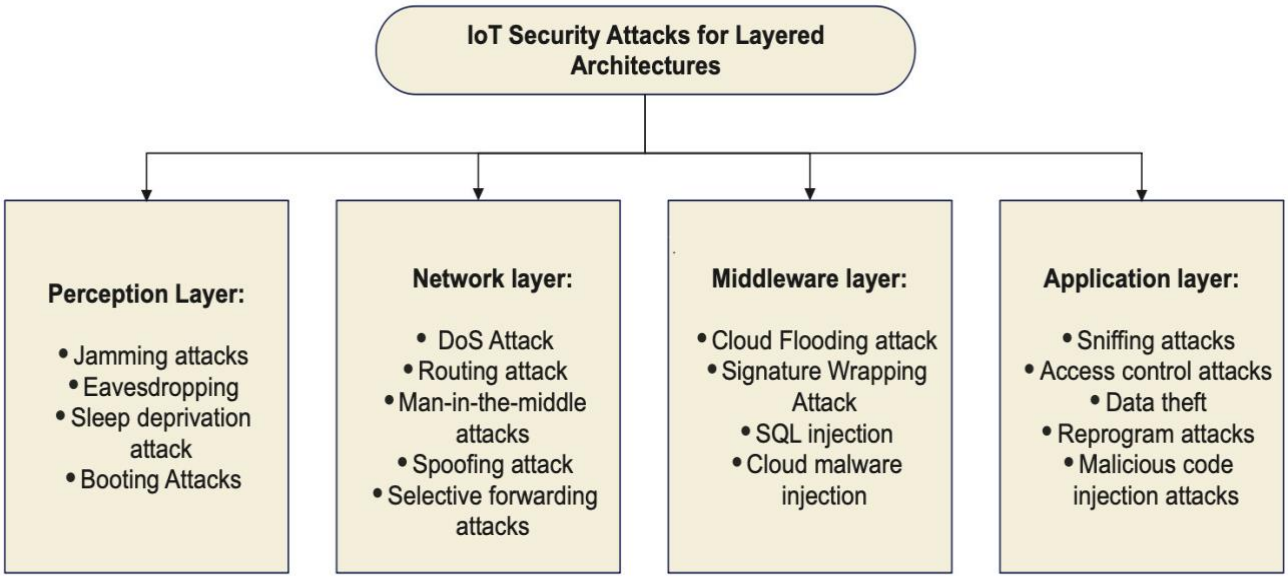

Figure 1. IoT Security Attacks for Each Layered Architecture

Perception Layer Attacks
The goal of many adversaries is to hack sensors that are actively gathering data in order to replace them with a malicious alternative. The following is a list of the most common forms of attacks that often target the perception layer.

Jamming attacks
Jamming attacks are one of the most common kinds of attacks used against devices operating on the perception layer. They create an issue by interfering with and halting communication, reducing the level of performance of IoT devices, and cutting down on the energy used by IoT devices [15]. There are a wide variety of jamming attacks, including reactive jammers, continual jammers, misleading jammers, and random jammers [14].

Eavesdropping
Because IoT apps are vulnerable to eavesdropping, there is a risk associated with this form of assault. Attackers are able to gain access to IoT devices and steal crucial information that is passed between the data tag and the data reader [11].

Sleep deprivation attack
The goal of this kind of assault is to deplete the energy supply of IoT edge devices over a long period of time. As a result, IoT nodes will be unable to offer any kind of service since the device will be forced to shut down due to increased battery power consumption [12].

Booting Attacks
It is possible to use it to perform a wide variety of harmful activities. Attackers can obtain access to devices and run malicious code because of vulnerabilities in reboot operating systems that exist on the edge of devices [17].

Network layer Attack

The issues of compatibility, privacy, and confidentiality are the most significant to consider when it comes to security in the network layer. The following are the most common kinds of network threats.

DoS Attack

This type of assault is one of the most common and most devastating attacks on a network. This is because it attempts to block users from gaining access to services and makes those services unavailable [16]. There are a variety of ways in which attackers can attack an RFID system, tag, or network, including by making the system inoperable or by making tags invisible to readers [14].

Routing attack

Routing attacks include many kinds of attacks, such as sinkhole attacks, wormhole attacks, Sybil attacks, and others, which attackers use in IoT systems. These attacks are used to change the proper routing path and the routing loop at any point in the data collection and transmission process [17].

Man-in-the-middle attacks

An adversary might launch the attack by eavesdropping on communication taking place between two IoT devices. The attacker has the ability to gain access to private data, take over the device, and change data without the owner's knowledge [12].

Spoofing attack

A type of assault known as "spoofing" is one in which an IP address, MAC address, or any number of other pieces of information are changed to cause disruptions in network traffic. This is done to gain unauthorized access to sensitive data and to generate bogus error messages [18].

Selective forwarding attacks

This kind of attack can be particularly risky in IoT networks because it is exceedingly difficult to both identify and prevent. As the attackers in this type of attack function as nodes in the communication system, they are able to selectively forward or drop particular packets that are sent via a network [4].

Middleware layer Attack

It is essential to have a middleware layer in IoT applications to provide strength and stability, but these layers are susceptible to a variety of attacks. The following is a description of the most typical kinds of attacks that occur on the middleware layer:

Cloud Flooding attack

This type of attack has an effect on the quality of the cloud system since the attackers utilize a continuous stream of requests to exhaust the resources provided by the cloud provider [17]. There is a problem with increased cloud utilization, which is the cloud not having the ability to differentiate between legitimate and attack traffic [12].

Signature Wrapping Attack

This kind of attack most often takes place in the middleware layer. Cloud services have a vulnerability that allows attackers to access the information, which also makes it possible for the attackers to break and change the information's substance by destroying the signature of the data [21].

SQL injection

The database is the target of this particular type of assault. An attacker can exploit the vulnerabilities of IoT devices to insert malicious code whenever there is any change in any user information, database records, or new instruction [1][9].

Cloud malware injection

This type of attack occurs when malicious malware is implanted into a cloud, allowing the attacker to take over the cloud and implant a virtual machine. To receive service, this virtual machine pretends to be a real one [20].

Application layer Attack

The application layer is faced with a range of challenges and problems with security, such as issues relating to data theft and privacy concerns [13]. IoT applications are the target of attackers' attention since it is easy to exploit vulnerabilities found in application layers [19]. The following are some instances of attacks on the application layer:

Sniffing attacks

An adversary can carry out this kind of assault on an IoT application by using specialized software to sniff or track network traffic to gain access to users' personal data and steal it [9].

Access control attacks

An access control attack is one of the greatest risks to IoT software. Access to the data or account can only be granted to those people or processes considered legitimate. When this access is compromised, the entire IoT system becomes more vulnerable [20].

Data theft

The attackers can intercept sensitive information through communication between devices. When information transmits through IoT devices, the data are vulnerable to assault. Encryption methods and correct authentication of all devices connected to a network are essential components of an IoT security strategy that are important to implement for protecting data on connected devices [21] [22].

Reprogram attacks

If IoT devices are not saved correctly, attackers can reprogram the devices, allowing them to take control of

the entire network [17]. By abusing the software system and injecting specific commands inside its programming, attackers can hack and reprogram the entire system [22].

Malicious code injection attacks

This type of attack occurs when inserting malicious code into the IoT system devices. The most straightforward approach for attackers to gain access to a system is by introducing malicious code into a script [23]. Also, it might insert hostile code into the memory of a node, which causes it to carry out operations not intended and allow it to take control of an entire IoT system [22].

5. IoT SECURITY AND ML

The field of ML has been gaining significant attention recently, as it has the potential to significantly enhance IoT security by enabling the rapid identification of threats and anomalies. ML can be used to secure IoT devices from cyberattacks because it is considered a unique solution compared to other traditional solutions. ML algorithms have a variety of applications that can be used for intrusion detection, malware detection, and other forms of detection. Several different ML approaches, such as classification and regression analysis, feature optimization approaches, rule-based techniques, and clustering, can be utilized to gain insights from data about the security of IoT devices [9]. The algorithms that make up ML can generally be categorized into one of the following four categories: supervised learning, unsupervised learning, semi-supervised learning, and reinforcement learning. Figure 2 shows ML and its classification. These algorithms can be used to develop a robust defense policy and identify assaults on devices connected to the IoT. This section explains the various ML algorithms utilized for IoT security systems.

Supervised learning

In ML, the method known as supervised learning is considered the most common. The algorithm is trained on a dataset that has been labeled. It does this by seeing examples of mappings between inputs and outputs that have been labeled. The purpose is to use the learned mapping to make predictions on data that have not yet been seen. Classification and regression are the two tasks that can be used for supervised learning algorithms [24].

A) Classification Learning

It is utilized for predicting future events and modeling existing datasets. The subsections provide an overview of a number of different classification methods, including the Bayesian Theorem, Support Vector Machine, Association Rule K-Nearest Neighbor, and Random Forest.

Support Vector Machines (SVMs)

It can be utilized for both classification and regression analysis. SVMs produce a hyperplane that splits data into different classes. The primary concept behind support vector machines is to raise the length between the hyperplane and the closest points of each class [12] [17]. SVMs have the ability to model non-linear decision boundaries by introducing new characteristics due to the utilization of kernel functions [4]. It is well suited to combat security challenges in the IoT because it has high accuracy [25]. SVM uses anomalous profiling behavior shown by IoT devices and identifies Android malware to ensure dependable IoT services [9].

Naïve Bayes (NB)

It is known as Bayesian Theorem, commonly referred to as a probabilistic classifier. Naive Bayes depends on previous information to calculate the probability of an occurrence [17]. It has a principal function for determining the classification of words in the text based on a training dataset that contains data with N-dimensional dimensions [29]. The Naive Bayes method has several benefits, such as its simplicity and ease of use and suitability for multiple classifications. It is applicable to implementing intrusion detection at the network layer and anomaly detection [4].

K-nearest neighbor (KNN)

Both classification and regression are possible applications of the KNN algorithm. In most cases, the Euclidean distance function is used by KNN classifiers because it is a nonparametric approach. The KNN algorithm calculates an average value for each new data point based on the Euclidean distance in which k points are its nearest neighbors [4]. While this approach is efficient to implement and has simple computation, it suffers from inaccuracy when dealing with massive data sets [25]. The KNN approach is used in the IoT for the purposes of detecting intrusions, malware, and anomalies [12].

Random Forest (RF)

The Random Forest method is among the most popular ML techniques for ensemble techniques to generate accurate results. It uses multiple DTs to construct an ensemble learning method for making predictions for a better overall outcome [17]. The RF algorithm has the merit of decreasing feature correlation between trees by randomly dividing the data into smaller samples, thereby making it more accurate than traditional decision trees [15]. RF is an efficient method when dealing with massive datasets [26], indicating that it can enhance IoT security and raise the accuracy of intrusion detection systems. Also, it is used for attacks, such as DDoS attack detection and identifying anomalies and unauthorized IoT devices [27].

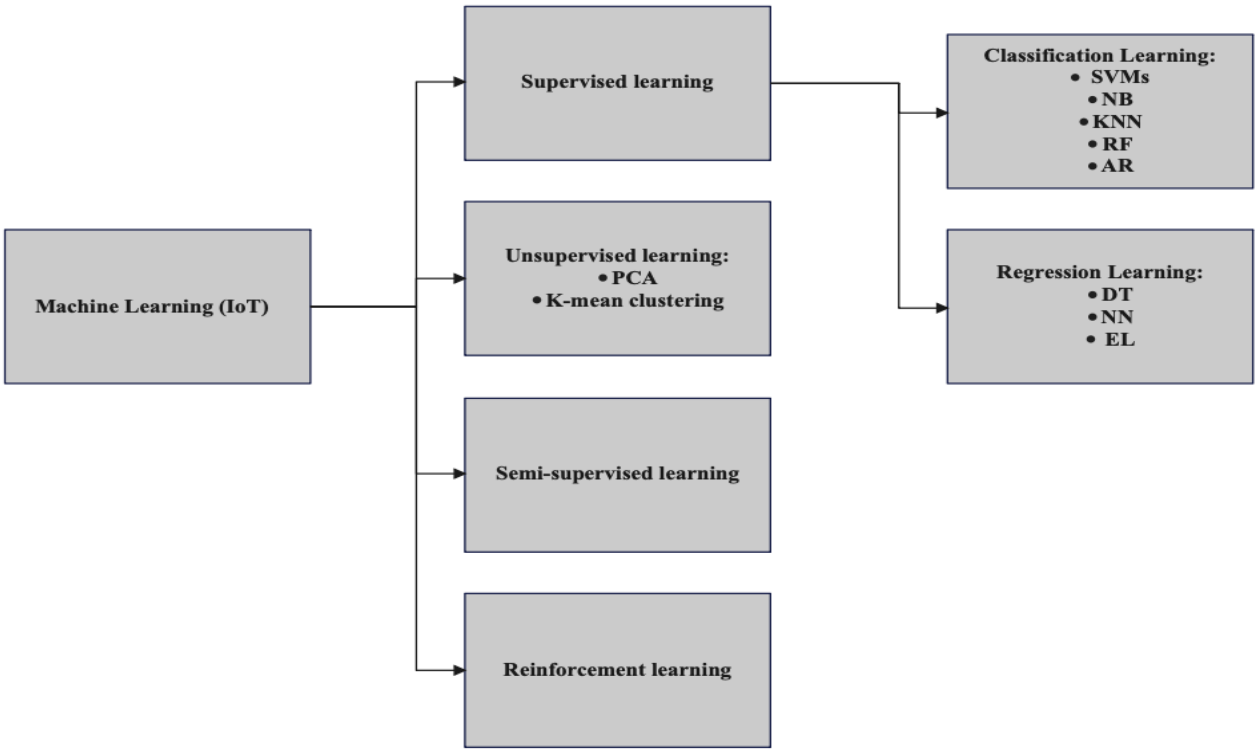

Figure 2. Machine Learning and its Classification

Association Rule (AR)

The purpose of the AR method is to identify connections among the unknown variables of the dataset to identify patterns and correlations. Thus, it can make new predictions for hidden relationships between variables [23]. It is utilized effectively to detect many types of attacks and intrusions [29]. The AR algorithm is generally considered as being easy and straightforward to implement, but it does not have accurate results in the IoT when using a large dataset because it depends on assumptions and high-level time of complexity [4]. The fuzzy AR algorithm is utilized as a detection method in the network system [30].

A) Regression Learning

Regression learning is used when the learned amount is an actual digit or constant value that relies on the input variables. The following subsections introduce several types of RL, including Neural Networks, Ensemble Learning, and Decision Trees.

Decision Tree (DT)

DTs are popular in ML methods and are mainly used for two types: classification and regression. A DT appears like a tree with branches and leaves [4]. A DT classifier aims to build a model that is utilized in selecting sample information and relies on the classification of feature values [30]. This algorithm has several benefits, such as being easy to interpret and use and its ability to handle significant values and give a clear representation. However, it has some disadvantages compared to other ML approaches; in particular, it needs a vast amount of storage due to its ample space [12]. It is used extensively within IoT network security to detect DDoS attacks and identify the source of malicious traffic [30].

Neural Network (NN)

NN has taken inspiration from the human brain in that it mimics the function and structure of biological neurons. Neural networks have the ability to solve complex situations and nonlinear issues [12]. There are two primary types of NN algorithms: hierarchical and interconnected. These types are based on the multiple functional levels of the neurons in the network, where each layer is responsible for a particular kind of issue or application [4]. Neural networks are a robust method for detecting threats of DoS attacks and other types of network intrusions [31]. However, NNs face various challenges while attempting to implement an IoT system because they are computationally difficult [25].

Ensemble Learning (EL)

EL is considered one of the newest, most exciting developments in recent advances in ML. It has uses in several applications due to its flexible and robust approach. EL is able to enhance classification performance by combining multiple output models of ML algorithms to get a more accurate and resilient predictive model [29]. The goal of EL is to get a set of prediction results by applying several types of multi-classifiers [4]. EL helps decrease the variance and overfitting of the

information due to having multiple different models [12]. EL has the ability to detect anomalies, intrusions, and viruses efficiently [17]. Also, it is utilized for the detection of malicious software on Android [30].

Unsupervised learning

This method only provides input variables, but it does not produce the desired outputs. The data are not required to have any labels. It attempts to determine the similarities present in the data set, so it classifies the data into a variety of categories known as clusters [24].

Principal Component Analysis (PCA)

PCA is classified to use widely on unsupervised ML methods. It is considered a statistical method used to analyze data to extract functional patterns and minimize the dimensionality of massive datasets while still preserving most of the features of information about datasets [33]. Also, it is used to determine the most significant subset of features that contributes to a particular classification [34]. PCA helps improve IoT security. By using PCA in IoT systems, it can use selecting features to implement IoT intrusion detection systems that operate in real time [17]. Using PCA and other ML techniques together provides a robust security mechanism and effective security protocol [4].

K-mean clustering

K-means clustering is a method utilized in the field of unsupervised ML. Clustering depends on the similarity of putting data points into groups to discover hidden structures and patterns in data. There is no requirement for any needed data to be labeled for training a model [32]. Supervised learning techniques have the ability to access the data label while they are being trained. Thus, they are considered more effective than K-mean clustering for detecting attacks [12]; however, K-means clustering is a popular algorithm to utilize for the detection of anomalies as well as Sybil attacks [4].

Semi-supervised learning

The semi-supervised learning technique exists between unsupervised learning and supervised learning. The model needs either entire labels for all the data or none during training. The cost of data labeling is a relatively expensive process [36]. The use of semi-supervised learning is rare in the field of IoT security because it may not be able to provide the same level of accuracy detection as supervised learning [29].

Reinforcement learning

It is among the most crucial areas of ML algorithms. RL is unable to interact with its surroundings without any prior information. The purpose of reinforcement learning is to attempt to learn a strategy that maximizes long-term rewards. The learning behavior is inspired by humans and animals [35]; therefore, it is a good option for robots to choose while making decisions for various tasks without needing pre-defined programming [36]. RL helps to improve intrusion detection in the IoT and provides a robust solution for protecting IoT networks. It can be used to resist attacks on IoT networks from hostile learning environments [28]. IoT security has used two reinforcement learning methods: Q-learning and Dyna-Q. Jamming threats, harmful inputs, and authentication are utilized for the Q-learning method, while malware and authentication are utilized for the Dyna-Q method [4].

In Table 2, we have summarized multiple machine-learning techniques that solve different security problems in IoT.

Table 2. Summary of machine learning techniques.

Reference paper	Model	Approach
[4]	NB	It can detect anomalies and intrusions network.
[4]	K-means	It commonly uses for anomaly and Sybil attack detection.
[9][25]	*SVMs*	It can fight IoT issues and detects Android malware.
[12]	KNN	It can identify malware, intrusions, and anomalies.
[17]	*PCA*	It assists in enhancing IoT security and detecting intrusion systems.
[17][30]	*EL*	It detects intrusions, anomalies, and viruses. It detects Android malware
[26][27]	RF	It can improve IoT security and detection systems. It can identify DDoS assaults and illegal IoT devices.
[30]	AR	It uses a fuzzy AR algorithm to detect network systems.
[30]	*DT*	It identifies DDoS attacks and finds malicious traffic in the network.
[31]	*NN*	It detects DoS attacks and different kinds of network intrusions

6. CONCLUSIONS

IoT technology has significantly improved the quality of people's lives, as IoT technologies help connect and access information from anywhere and anytime. Although the IoT has brought several advantages to people's lives and improved accessibility and efficiency, the aspect of security is becoming a more significant concern in the whole IoT system. IoT devices and network systems are increasingly vulnerable to assaults and other security issues, so increasing and enhancing security and safety is

essential. The advancement of ML and other technologies allows IoT security to develop and better address security risks.

In this survey, we have delivered an overview of IoT security. A review of some recent related work is also demonstrated. We have highlighted basic architectural information and several security vulnerabilities and attacks at four architecture layers of IoT security. We have discussed in detail solutions to IoT security threats, such as ML, which presents a solution for mitigating IoT security risks.

7. REFERENCES

[1] Ghaida Alqarawi, Bashayer Alkhalifah, Najla Alharbi & Salim El Khediri (2022) Internet-of-Things Security and Vulnerabilities: Case Study, Journal of Applied Security Research, DOI: 10.1080/19361610.2022.2031841

[2] Harbi, Y., Aliouat, Z., Harous, S., Bentaleb, A., & Refoufi, A. (2019). A review of security in internet of things. Wireless Personal Communications, 108, 325-344.

[3] Mohanta, B. K., Jena, D., Satapathy, U., & Patnaik, S. (2020). Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet of Things, 11, 100227

[4] Tahsien, S. M., Karimipour, H., & Spachos, P. (2020). Machine learning based solutions for security of Internet of Things (IoT): A survey. Journal of Network and Computer Applications, 161, 102630.

[5] HaddadPajouh, H., Dehghantanha, A., Parizi, R. M., Aledhari, M., & Karimipour, H. (2021). A survey on internet of things security: Requirements, challenges, and solutions. Internet of Things, 14, 100129.

[6] N. Mishra and S. Pandya, "Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review," in IEEE Access, vol. 9, pp. 59353-59377, 2021, doi: 10.1109/ACCESS.2021.3073408

[7] Williams, P., Dutta, I. K., Daoud, H., & Bayoumi, M. (2022). A survey on security in internet of things with a focus on the impact of emerging technologies. Internet of Things, 19, 100564.

[8] Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., & Arshad, H. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. Computers & Security, 112, 102494.

[9] Sarker, I.H., Khan, A.I., Abushark, Y.B. et al. Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions. Mobile Netw Appl (2022). https://doi.org/10.1007/s11036-022-01937-3

[10] Khattak, H. A., Shah, M. A., Khan, S., Ali, I., & Imran, M. (2019). Perception layer securityin internet of things.Future Generation Computer Systems,100, 144–164.https://doi.org/10.1016/j.future.2019.04.038

[11] R. Khader and D. . Eleyan, “Survey of DoS/DDoS attacks in IoT”, Sustainable Engineering and Innovation, vol. 3, no. 1, pp. 23-28, Jan. 2021

[12] Shara, J., & Gjirokaster, A. A REVIEW ON IOT SECURITY USING ML&DL.

[13] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," in IEEE Access, vol. 7, pp. 82721-82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

[14] Khattak, H. A., Shah, M. A., Khan, S., Ali, I., & Imran, M. (2019). Perception layer security in Internet of Things. Future Generation Computer Systems, 100, 144-164.

[15] Ahmad, R., & Alsmadi, I. (2021). Machine learning approaches to IoT security: A systematic literature review. Internet of Things, 14, 100365.

[16] I. Butun, P. Österberg and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures," in IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 616-644, Firstquarter 2020, doi: 10.1109/COMST.2019.2953364

[17] Bharati, S., & Podder, P. (2022). Machine and deep learning for iot security and privacy: applications, challenges, and future directions. Security and Communication Networks, 2022, 1-41.

[18] Jayalaxmi, S., & Siddharth, S. IOT APPLICATIONS SECURITY ISSUES AND SOLUTIONS–A STUDY.

[19] Sohn, N., Bashir, N., & Plantz, M. Potential Research Challenges of ML and DL based IoT security Schemes.

[20] V. -D. Gavra, I. -M. Dobra and O. A. Pop, "A Survey on Threats and Security Solutions for IoT," 2020 43rd International Spring Seminar on Electronics Technology (ISSE), Demanovska Valley, Slovakia, 2020, pp. 1-5, doi: 10.1109/ISSE49702.2020.9120977.

[21] P. K and B. Nataraj, "Certain Investigation of Attacks in the Field of Internet of Things and Blockchain Technology," 2022 Smart Technologies, Communication and Robotics (STCR), Sathyamangalam, India, 2022, pp. 1-6, doi: 10.1109/STCR55312.2022.10009205.

[22] N. A. Khan, A. Awang and S. A. A. Karim, "Security in Internet of Things: A Review," in IEEE Access, vol. 10, pp. 104649-104670, 2022, doi: 10.1109/ACCESS.2022.3209355.

[23] Srinadh, V., Rao, M. S., Sahoo, M. R., & Rameshchandra, K. (2021, March). An analytical study on security and future research of Internet of Things. In Materials Today: Proceedings.

[24] Haji, S. H., & Ameen, S. Y. (2021). Attack and anomaly detection in iot networks using machine learning techniques: A review. Asian journal of research in computer science, 9(2), 30-46.

[25] S. Gupta, S. Vyas and K. P. Sharma, "A Survey on Security for IoT via Machine Learning," 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA), Gunupur, India, 2020, pp. 1-5, doi: 10.1109/ICCSEA49143.2020.9132898.

[26] Alsamiri, J., & Alsubhi, K. (2019). Internet of things cyber attacks detection using machine learning. International Journal of Advanced Computer Science and Applications, 10(12) doi:https://doi.org/10.14569/IJACSA.2019.0101280

[27] Y. Baja and K. Chougdali, "Security of Internet Of Things Using Machine Learning," 2022 9th International Conference on Wireless Networks and Mobile Communications (WINCOM), Rabat, Morocco, 2022, pp. 1-6, doi: 10.1109/WINCOM55661.2022.9966417.

[28] A. Uprety and D. B. Rawat, "Reinforcement Learning for IoT Security: A Comprehensive Survey," in IEEE

Internet of Things Journal, vol. 8, no. 11, pp. 8693-8706, 1 June1, 2021, doi: 10.1109/JIOT.2020.3040957.

[29] 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," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1646-1685, thirdquarter 2020, doi: 10.1109/COMST.2020.2988293.

[30] Thakkar, Ankit, and Ritika Lohiya. "A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges." Archives of Computational Methods in Engineering 28 (2021): 3211-3243.

[31] K. R. Dalal, "Analysing the Role of Supervised and Unsupervised Machine Learning in IoT," 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2020, pp. 75-79, doi: 10.1109/ICESC48915.2020.9155761

[32] Datti Emmanuel Useni , Abdulsalam Ya'U Gital , Okere Chidiebere Emmanuel, Goteng Kuwunidi Job , Abuzairu Ahmad, 2023, A Review of Machine Learning-based Algorithms for Intrusion Detection System, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 12, Issue 01 (January 2023),

[33] Yulianto, A., Sukarno, P., & Suwastika, N. A. (2019, March). Improving adaboost-based intrusion detection system (IDS) performance on CIC IDS 2017 dataset. In Journal of Physics: Conference Series (Vol. 1192, No. 1, p. 012018). IOP Publishing.

[34] Saheed, Y. K., Abiodun, A. I., Misra, S., Holone, M. K., & Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. Alexandria Engineering Journal, 61(12), 9395-9409.

[35] F. Hussain, R. Hussain, S. A. Hassan and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1686-1721, thirdquarter 2020, doi: 10.1109/COMST.2020.2986444.

[36] Farooq, U., Tariq, N., Asim, M., Baker, T., & Al-Shamma'a, A. (2022). Machine learning and the Internet of Things security: Solutions and open challenges. Journal of Parallel and Distributed Computing, 162, 89-104.