Journal of
Sensor and Actuator Networks

MDPI

Article

Safety, Security and Privacy in Machine Learning Based Internet of Things

Ghulam Abbas [1], Amjad Mehmood [2,3,*], Maple Carsten [2], Gregory Epiphaniou [2,*] and Jaime Lloret [4]

[1] Department of Computer Science, National University of Modern Languages, H-9, Islamabad 44000, Pakistan; abbasfacho@gmail.com
[2] Warwick Manufacturing Group (WMG), University of Warwick, Coventry CV4 7AL, UK; cm@warwick.ac.uk
[3] Institute of Computing, Kohat, University of Science & Technology, Kohat 46000, Pakistan
[4] Integrated Management Coastal Research Institute, Polytechnic University of Valencia, Camino Vera s/n, 46022 Valencia, Spain; jlloret@dcom.upv.es
* Correspondence: dramjad.mehmood@ieee.org (A.M.); gregory.epiphaniou@warwick.ac.uk (G.E.)

Abstract: Recent developments in communication and information technologies, especially in the internet of things (IoT), have greatly changed and improved the human lifestyle. Due to the easy access to, and increasing demand for, smart devices, the IoT system faces new cyber-physical security and privacy attacks, such as denial of service, spoofing, phishing, obfuscations, jamming, eavesdropping, intrusions, and other unforeseen cyber threats to IoT systems. The traditional tools and techniques are not very efficient to prevent and protect against the new cyber-physical security challenges. Robust, dynamic, and up-to-date security measures are required to secure IoT systems. The machine learning (ML) technique is considered the most advanced and promising method, and opened up many research directions to address new security challenges in the cyber-physical systems (CPS). This research survey presents the architecture of IoT systems, investigates different attacks on IoT systems, and reviews the latest research directions to solve the safety and security of IoT systems based on machine learning techniques. Moreover, it discusses the potential future research challenges when employing security methods in IoT systems.

Keywords: internet of things (IoT); machine learning; security and privacy; CPS

Citation: Abbas, G.; Mehmood, A.; Carsten, M.; Epiphaniou, G.; Lloret, J. Safety, Security and Privacy in Machine Learning Based Internet of Things. *J. Sens. Actuator Netw.* **2022**, *11*, 38. https://doi.org/10.3390/jsan11030038

Academic Editor: Mingjun Xiao

Received: 11 June 2022
Accepted: 15 July 2022
Published: 29 July 2022

1. Introduction

The miraculous advancement in the Internet of Things (IoT) has led to one of the fastest developing computing paradigms, with an estimated of 75 billion smart devices by the end of 2025 [1] It can collect, classify, comprehend and respond to its environment [2]. IoT plays an important role in improving smart systems, such as education, homes, agriculture, farming, grid, transportation, etc. [3,4]. The adoption of this new technology has led to a number of benefits, such as efficiency, productivity, new business directions, agility and mobility and, most importantly, cost reductions. However,the increasing demand and growing deployment of IoT has led to serious new security challenges [5]. IoT systems consist of integrative arrangements of devices, which makes the system very complex, and most IoT system works in an unsolicited and unattended environment. The devices that typically connect over wireless networks in IoT are often targeted by hackers and intruders, eliciting secret information using phishing, eavesdropping, denial of service, spoofing, obfuscation and jamming faces [6–9]. Therefore, the security risk in an IoT system is higher than that for other computing paradigms, and traditional methods may not be effective in overcoming these security issues. Hence, maintaining and managing the security of the IoT system is very challenging task. A holistic solution is needed to satisfy the security requirements of the IoT system. The existing security methods, such as authentication, encryption, network security and access control, are more challenging and inadequate for large IoT systems with a number of controlling devices. For instance, in DDoS, the attacks

spoofed the source IP addresses to attack a location and the legitimate users struggled to access their IoT devices due to the systems' vulnerabilities. Machine Learning algorithms have a unique way of solving complex problems that are implemented in many real-time applications [10]. The basic aim of machine learning algorithms is to improve the performance of any task through training and experience, and it can assess the large dataset with an extraordinary analytical ability in any cyber-physical system [11,12]. It has been used in many fields, including autonomous vehicles, medicine, image recognition, etc.

The research contributions of this survey are as follows:

- A detailed discussion on the attack surfaces, vulnerabilities, and security threats of IoT Systems: we discuss various attack surfaces on IoT devices, i.e., network, physical service, cloud service, application interfaces and web service.
- Detailed discussion and comparison of existing surveys, including an in-depth statistical overview of recently published articles on different ML techniques for IoT security.
- Incorporation of recent surveys on financial losses by breaches in the security of IoT systems, including the trend in the number of IoT devices in future.
- Presentation of the latest research challenges and future directions for IoT security based on ML.

The rest of the paper is organized as follows: Section 2 presents the related works on the topic. Section 3 demonstrates the safety and security threats in IoT. Machine learning techniques and their applications in IoT are presented in Section 4. Issues, research challenges, and future research directions are mentioned in Section 5. Section 6 presents a discussion of the observations and results. Finally, the conclusion is given in Section 7.

2. An Overview of IoT System

The Internet of Things (IoT) consists of a cyber-physical system, randing from small sensors to global positioning systems and near-field communication sensors to radio-frequency identification devices (RFID), including emergency alarms and detectors [13]. All these IoT devices collect, classify, communicate, comprehend, and respond to their environment in real-time. These devices are used to store all types of information, such as light intensity, sound data, electricity consumption, temperature readings, chemical reactions, biological changes, etc. The IoT structure is the interconnection of a heterogeneous cyber-physical system in diverse communication forms, such as machine-to-machine interconnection, man-to-man communication, and machine-to-man interactions.

The main task of the IoT system is to convert the conventional object to a smart object using intelligent devices and processes, such as sensor networks, pervasive computing, internet protocols, communication technologies, and applications. The IoT model consists of physical devices, which interact and integrate with communication networks to deliver smart services and applications. The architecture of the IoT system can be divided into three layers, i.e., application, network, and a presentation or physical layer [14]. The architecture and analysis of IoT is shown in Figure 1.

The three-layer IoT architecture shown in Figure 1 defines the main idea of the IoT system, which is also summarised as follows:

1. The presentation or physical layer consists of all the physical objects that are responsible for sensing and collecting information from its surrounding environment. The sensors in this layer identify smart objects in the environment.
2. The network layer consists of connectivity devices and is responsible for connecting and communicating with smart objects, servers, and network devices. Features of this layer are used for communicating and processing the sensor data.
3. The application layer describes the various collaboration, deployments, and applications of IoTs such as smart objects for homes, transport, cities, agriculture and farming, etc. This layer classifies the application's services to a user.

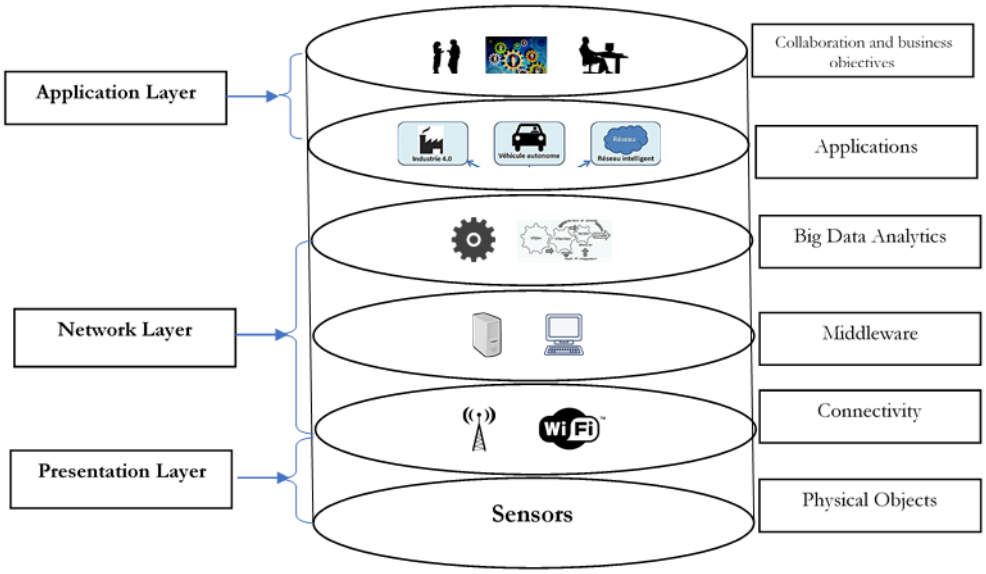

Figure 1. Architecture of IoT.

3. Safety and Security Threats in IoT

IoT integrates physical objects and their surroundings via internet connection. The devices primarily work in an unsolicited and unwanted online environment. Therefore, intruders and attacker may exploit the vulnerable IoT devices and expose private information and credentials from sensors by eavesdropping [15,16]. The threats can be classified as passive threats and active threats. Passive threats attempt to use data and information from the system but do not affect the system's resources, e.g., eavesdropping. Active threats refers to the attempts of an attacker/hacker to alter the data and take control of the hardware. Active threats include Sybil, denial of service (DoS), distributed denial of services (DDoS), Trojans, spoofing, phishing and smishing [17]. The potential security attacks that may affect the security requirements, i.e., authorisation, authentication, confidentiality, availability, integrity, and non-repudiation, are shown in the following Figure 2.

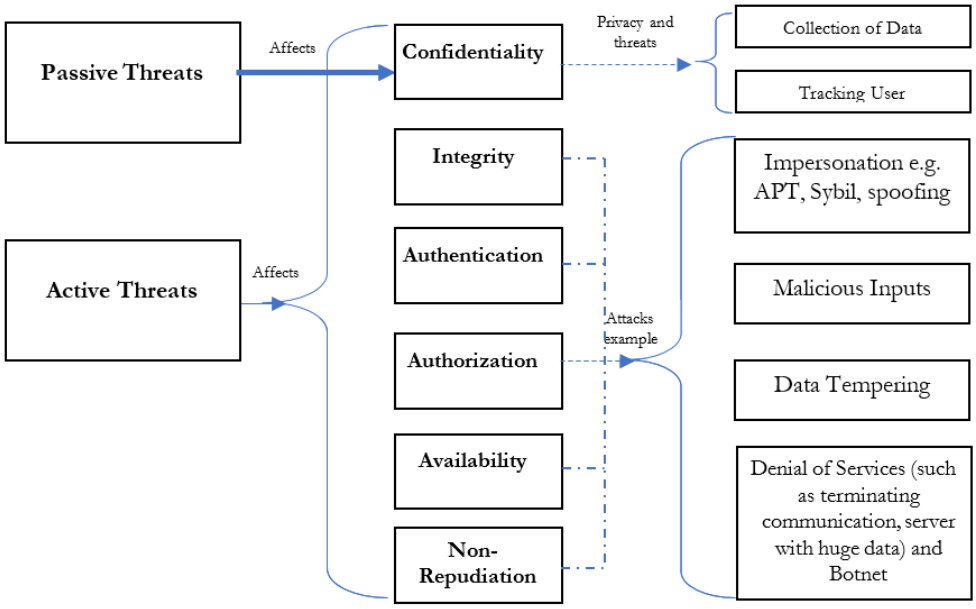

Figure 2. Type of security threats in IoT.

3.1. IoT Attack Surface(s)

Possible attack surfaces and potential threats are discussed in this section. The attack surfaces of IoT can be divided into network service, physical device, web and application services and cloud service, as shown in shown in Figure 3.

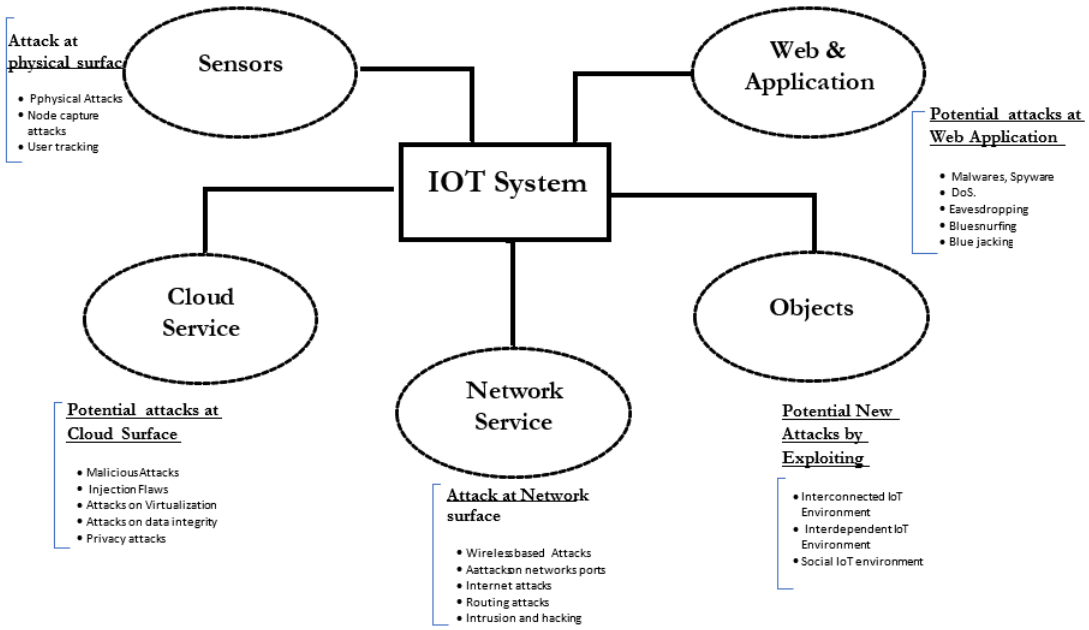

Figure 3. IoT Surface Attacks.

3.1.1. Attack Surface at Physical Devices

The physical surfaces are the primary means of cyber-physical threats. This IoT surface consists of sensors, RFIDs, and actuators.The sensors are used to collect all types of data from the IoT environment. RFIDs play an important role in wireless network communication through automatic identification with a unique identifier. This surface is physically reachable and most vulnerable to physical threats. Most physical devices have valuable information and are resource-constrained, making them a potential attack surface. For instance, physical devices can track device information by access requests, which may cause threats such as DoS, DDoS or other cyber-attacks [18].

3.1.2. Attack Surface at Network Service

The network service of an IoT system consists of two main parts, i.e., RFID and WSN [19]. Both parts are vulnerable to cyber threats: possible attacks on RFID at the presentation layer include Sybil, synchronization attack, and reply attacks; possible attacks at the network layer are false routing and eavesdropping; possible attacks at the application layer are buffer overflow and injection attacks. The possible attacks on the network layer of WSN include the Sybil attack, jamming and replay attacks. These security threats arises when the IoT system is directly integrated with traditional networks as the traditional networks system are no longer secure [17–19].

The routing protocol is another potential attack surface on the IoT network service, which may face serious security threats. Therefore, a secure routing protocol is necessary for a safe and secure IoT system. Attackers can also attack open ports and obtain information such as MAC, the router's IP address and the network gateway [20].

The following graphs shows IoT device trends and cyber security losses to the global markets. Figure 4 shows the number of IoT devices in the last two years i.e., 2020 and 2021, and a projected estimate of there being more than 75 billion devices by 2025. The next graph, in Figure 5, presents the average losses on the global market that were caused by

cyber security attacks in the last four years. This is expected to reach 8000 (USD) million losses in the year 2022 (source from Satsista.com).

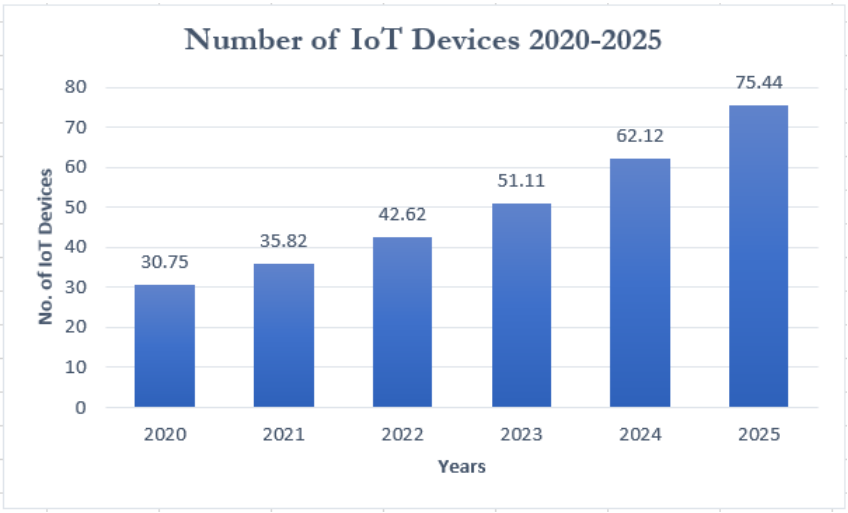

Figure 4. Number of IoT devices and projections up to 2025.

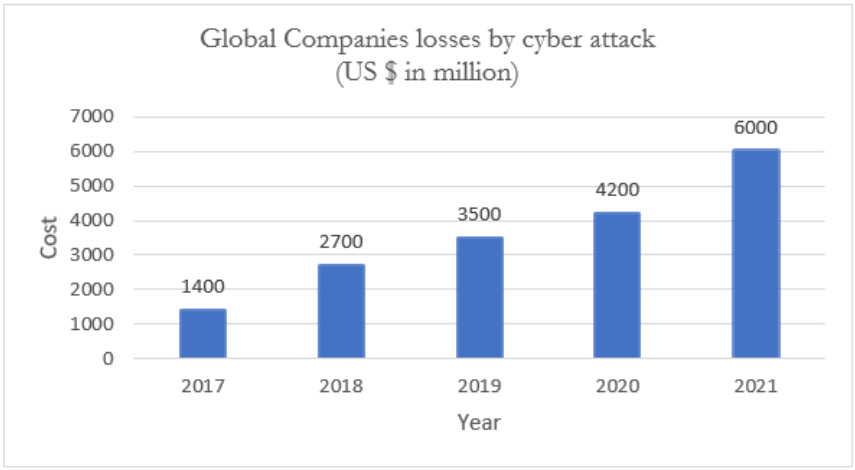

Figure 5. Global market losses by Cyber Attacks in the last five years.

3.1.3. Attack Surface at Cloud Service

Cloud computing provides a distributed service to the store and can obtain information at any time and anywhere [21]. The integration of the cloud-computing paradigm and IoT offers great opportunities for efficient IoT systems. However, several security issues arise with this integration, as the distributed system is more vulnerable to various cyber-security threats, such as: (a) Malicious attacks that manipulate flaws in data security by unauthorized access, e.g., cross-site scripting, SQL injection, cross-site requests [22]. (b) Inadequate integrity controls at the data level may face security threats. (c) The security threats in visualisation software may be used for malicious attacks, e.g., a weak authentication of a virtual server may permit a guest-operating system to run the codes. Privacy and security risks differ in cloud services as per the terms and conditions between the cloud user and service provider [22]. This integration may also introduce several privacy concerns by exposing personal and confidential information, e.g., personal home-based sensor data, medical data and reports, etc. To ensure the secure and reliable integration of cloud services and IoT systems, it is necessary to minimize possible cyber attacks [22,23].

3.1.4. Attack Surface at Web and Application Surface

Most IoT systems provide remote access services to users using Web-based or mobile applications. Smartphones and android-based systems became popular and captured a huge market due to the use of open architecture APIs among developers and malware developers. This permits users to access applications, including malicious online applications, which can store data without any security checks [24]. The malware designer can hack IoT-based systems by extracting device information and potential vulnerabilities, and creating botnets. The android applications may leak the user's privacy and private information, which can expose security risks such as blue-jacking, eavesdropping, smishing, blue-snaring, tracking, and DDoS [24].

4. Machine Learning for IoT Security

Machine Learning (ML) algorithms have a unique way of solving the complex problems implemented in many real-time applications [25]. The basic aim of machine learning algorithms is to solve complex tasks and improve the performance using training and experience. The ML algorithms automatically develop and control machines through experience with low-computational costs [26]. In this section, we first see the ML techniques in detail, then discuss the application of these algorithms in the field of IoT security. At the end of the section, other emerging techniques for IoT security will be briefly discussed.

4.1. Machine Learning (ML) Techniques

The machine learning (ML) algorithms are categories into supervised, unsupervised, and reinforcement learning.

4.1.1. Supervised Machine Learning

The supervised machine learning algorithms learn from experience with the labelled training data. They analyze the training data and imply a function that may be used to map new data samples. Supervised learning can be categorized into classification and regression. The dataset in the classification category is finite and can be binary, such as anomaly detection, or multitudinous, such as speech and face recognition, etc. The regression technique is used to identify the relationship between one dependent variable and another one, or more independent variables, which is often used to predict future outcomes.

4.1.2. Unsupervised Learning

In unsupervised learning, all the input data and samples are unlabeled. The trained model in this learning will not rely on input–output classes. The learning process can be defined as dimensionality reduction, clustering, and density estimation. The clustering method is used to group data in mathematical and statistical problems. This method is useful for unforeseen instances, such as unclassified data from any source [27].

4.1.3. Re-Inforcement Learning

Re-inforcement learning (RL) is considered between the supervised learning and unsupervised learning with no label information. RL is associated with reward value for good decision-making and maximising the rewards. There are two methods of doing this: value function approximation and policy search [28].

4.2. Application of Basic Machine Learning (ML) Techniques

This section discusses the most commonly used machine learning techniques.

4.3. Supervised Machine Learning

The most common supervised Machine Learning approaches are decision trees (DT), Bayesian algorithms, k-nearest neighbor (KNN), support vector machines (SVM), random forest (RF), and the association rule (AR). The graph shown in Figure 6 shows the research

paper statistics for different machine learning algorithms published in different publications up to December 2020.

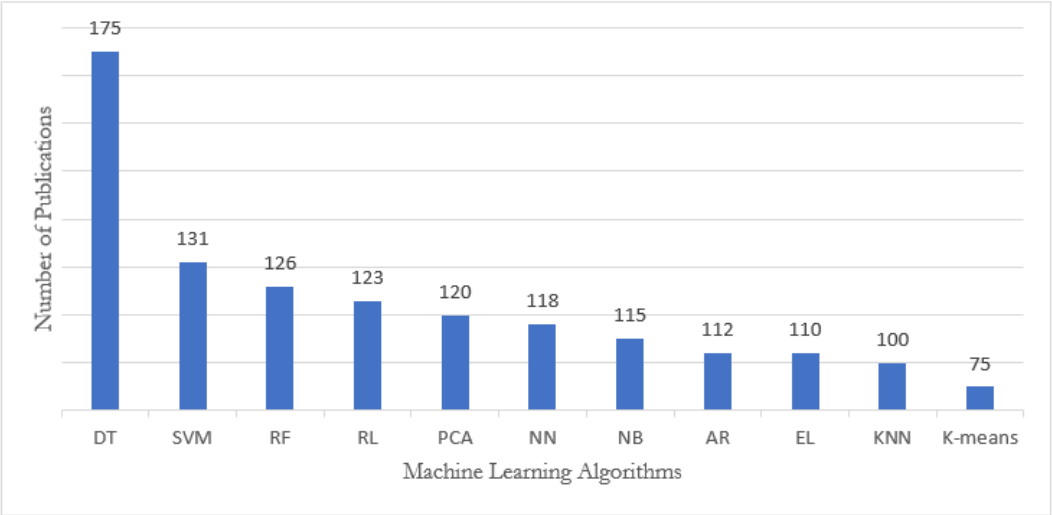

Figure 6. Research papers published on different Machine Learning algorithms up-to Dec. 2021.

4.3.1. Decision Trees (DTs)

This method classifies the sample dataset by sorting the feature values accordingly. Each node (vertex) of the tree represents a feature; each branch (edge) represents the value of a sample space to be classified. The sample data are classified as starting from the origin node of their feature, which optimally divide the sample space. This is considered as the origin node [29,30]. There are several ways of finding the optimal solution of the feature that splits the training samples. Entropy is a theory metric, used to measure the uncertainty in a group of observations. The following formula is used to calculate entropy when data are incorrectly classified [30]:

$$\sum_{n=1}^{c} -p_i log_2(p-i) \quad (1)$$

p_i is the probability of the data classifying to a given class of C. The lowest value of entropy used for root node.

There are two main phases in the DT approach, i.e., building and classification. In the building phase, the DT is constructed with unoccupied branches and nodes.The features splits the sample data until the leaves are obtained. In the classification phase, a tree is constructed with new samples of unknown features and the class proceeds along the path of corresponding values at the inner nodes [31]. The process is continued until a leaf is obtained. Accordingly, at the end of the process, the predicted classes are found [32].

The DT process can be simplified in five steps, as follows: (1) applying the pre- and post-pruning to reduce the size of the tree, (2) adjusting the space after the search state, (3) applying the search algorithm, (4) reducing the data features by removing the replicated features and (5) converting the trees into an appropriate data structure for further data operations. The DT approach uses machine learning classifiers to ensure the security and safety of data, such as DDOs and intrusion detection, and to detect suspicious traffic sources in a network [33,34]. There are some limitations to DT approaches, which can be simplified as follows: (1) the complex nature of the construction of a tree, which requires a large storage space, (2) DT-based approach is only feasible when few DTs are involved and becomes very complex when more DTs are involved, and (3) the computational cost with a complex model to implement.

4.3.2. Support Vector Machine

This method is used for the classification of datasets by constructing a hyperplane in the attributes among more classes. The distance between the hyperplane and the most adjacent attribute in each class needs to be maximized for the best classification of sample data [35]. The hyperplane that separates the data is expressed as:

$$a.x + b = 0 \tag{2}$$

where a is the particular vector, x is the feature vector and b is bias. The components of the equation can be written as $a^1.x^1 + a^2.x^2 + a^3.x^3 \ldots a^n.x^n$, n is number of vector dimensions x. The following equation is used to predict the vector [36,37]:

$$y = sign(ax - b) \tag{3}$$

the sign function returns -1 or $+1$ for negative or positive values, respectively. This classification method is familiar due to its suitability and capability for datasets with many feature attributes [36]. The main advantages of this approach include to performing real-time tasks and dynamically updating the particular dataset.

The SVM approach is generally used in safety and security applications. It is also proficient for storage applications, as it creates a hyperplane to divide the dataset points with less time and lower cost complexity [37–39].

A study conducted in [40] for the application SVM to secure the IoT system applied a linear SVM for malware detection. These are used to compare the performance and efficiency of SVM techniques with other learning algorithms for intrusion detection. The results obtained from many research studies showed that the SVM technique is more accurate and outperformed other learning techniques.

In [41], an SVM approach to device security, by transferring and receiving secure data and the results, showed that this is more effective for safe cryptographic techniques than the traditional method.

4.3.3. Bayesian Algorithms

This algorithm is used to calculate the probability of an event based on historical results. It can also be used to estimate and evaluate the probability of attack in a network traffic attack using previous network traffic information [42].

The NB classifier is treated independently of the features used for traffic classification, such as duration, connection, connection status flag, and connection protocol, e.g., UDP and TCP [43]. NB classification is used for intrusion and anomaly detection in any network traffic [43,44]. This classifier is more useful due to its simplicity and ease of implementation, low training data requirements, multi-class classification, and the robustness of its features. However, the NB classifier cannot capture useful hints from the interaction and relationships between features, which are important for classification [45].

4.3.4. K-Nearest Neighbor (KNN)

This is a non-parametric approach used for the classification of data samples, as shown in Figure 7. As per sample classification, there are three types of circular dots in the classified order. The green dots represent normal behavior, the red dots represents malicious behaviors, and unknown data samples, i.e., blue dots represent both normal and malicious behavior. Samples of an unknown class are decided according to the majority number in its nearest neighbors. To check and verify the results, a cross-validation is also used to test the different k values [46,47] The optimal value always varies depending on data samples, and finding the optimal value can be a time-consuming and challenging task. This approach is also used in intrusion and anomaly detection [48,49].

In [50], KNN is used for intrusion detection by classifying the nodes in a wireless sensor network regarding both normal or abnormal system behaviour. The proposed anomaly detection system shows accurate and efficient intrusion detection for an IoT environment.

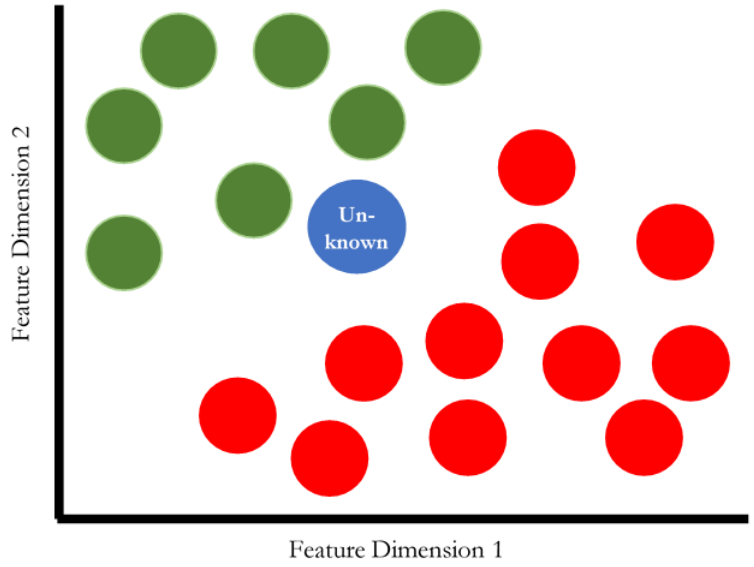

Figure 7. KNN classification principle.

4.3.5. Random Forest (RF)

This is an ensemble approach, which is used to predict the result based on the Decision Trees. The RF algorithm is mostly used for anomaly detection and intrusion detection [51]. The RF provided better classification results than other classifier algorithms, such as SVM, KNN and ANN, in case limited feature datasets are available. The RF uses the features achieved from network traffic to correctly recognize IoT devices. The researcher extracted network data from seventeen (17) IoT nodes, which are divided into nine categories to train the classifier using the RF algorithm. The research study conducted in [51,52] concluded that RF holds more practical importance for correctly identifying the unauthorized IoT devices compared to other ML algorithms.

4.3.6. Association Rule Algorithms

Association Rule (AR) algorithms are used to classify the unknown data and variables in the training dataset by examining the relationship variables. For instance, let P, Q and R be the variables dataset. The AR algorithm uses these variables and discovers their relationship, then constructs a model for the dataset [53]. This approach is not generally used in IoT safety and security systems as compared to other ML methods; however, the AR approach can be used by other ML algorithms to efficiently and effectively ensure IoT security. The disadvantage of AR algorithms is their high time complexity.

4.3.7. Ensemble Learning (EL)

This is a promising learning algorithm to produce a collective of basic classification methods, which can be used to improve the classification performance of a data sample. The main aim of the EL method is to combine the multi-classifier with heterogeneous or homogeneous data to obtain the best result [54]. An experimental assessment in [55] evaluated that EL is the best machine learning method according to application. A research study in [56] concluded that the time and cost complexity can be reduced for limited hardware resources in IoT devices. The main aim of the framework is to tackle issues such as, (1) distributed and automated online learning methods to identify the anomalies, and (2) help in assessing and obtaining the real data [56].

4.4. Unsupervised ML

In the following section, we discuss the general unsupervised machine learning approaches and their applications in IoT security, as well as their advantages, and disadvantages.

4.4.1. K-Means Clustering (KMC)

The KMC is an unsupervised machine learning approach, which is used to discover the clusters in any dataset. Clustering applies an iterative process to generate an accurate output. The input clusters consist of a set of dataset features. In the first step, the k centroid is calculated to assign the closest centroid cluster by calculating the distances between the points using Euclidean distance. Then, the cluster centroids are recalculated using the mean of samples assigned to one particular cluster. The same method is repeated until no clusters exist in the dataset [57]. The KMC approach is applied to the network detection of anomalies by classifying abnormal behavior [58]. In [59], k-means clustering is used to detect anomalies in an IoT system. Unsupervised algorithms have numerous applications in the safety and security of IoT systems. A study in [60] showed that KMC method has the ability to protect private data anonymization in an IoT environment. This clustering method is used to develop an algorithm of data anonymization for advance data-exchange security. The limitation of this approach is the selection value of k, assuming the clusters have approximately the same numbers in the dataset.

4.4.2. Principal Component Analysis

This is an unsupervised algorithm for the feature reduction of large data into reduced data that have the same information that was embodied in the large set. The convergence of the number of correlated and reduced to uncorrelated features is known as principal components. The PCA principle can be applied to real-time intrusion and anomaly detection [61]. The combination of PCA and other ML classifier methods, such as KNN and SVM, provide an efficient and secure computing system, which may be used in the real-time IoT system.

The research survey is summarized in the following Table 1, a comparison of different research studies on the safety and security of IoT based on machine learning algorithms.

Table 1. Comparison of ML Algorithms for IoT security.

Ref.	Supervised Learning							Unsupervised ML		Threat Detected
	NB	SVM	DT	KNN	RF	AR	EL	K-Means	PCA	
[60]	-	√	-	√	-	-	√	-	-	False detection attack
[62]	-	√	-	-	-	-	-	-	-	Intrusion detection
[63]	-	-	-	-	√	-	-	-	-	Authorization
[64]	-	-	-	-	-	-	-	-	√	Intrusion detection
[65]	-	√	-	-	-	-	-	-	-	Authentication
[66]	-	-	-	-	-	-	√	-	-	Authorization
[67]	-	-	-	√	-	-	-	-	-	Impersonation attack
[68]	-	√	-	-	-	-	-	√	-	Data tempering
[69]	-	-	-	-	-	-	-	-	√	Intrusion detection
[70]	-	-	-	-	-	-	-	-	-	Intrusion detection

4.5. Emerging Techniques for IoT Safety and Security

Federated machine Learning and Generative Adversarial Network are the latest field of machine-learning, which have opened new research areas. In the following sections, we will briefly shed light on the emerging machine learning techniques:

4.5.1. Federated Learning (FL)

Federated machine learning is a decentralised collaborative learning technique and is used to gain more experience from large datasets at different locations. The main property of federated machine learning is to secure the data that are collected through different mediums. In contrast with other approaches, FL allows for the model to transfer, without removing data from their origin [71]. This feature makes FL a good choice for IoT systems in terms of privacy and security. Federated learning overcomes the massively distributed

and private datasets, which create challenges in ML, by enabling on-device ML, without the migration of private end-user data to any central cloud.

4.5.2. Generative Adversarial Network (GAN)

This is a deep machine-learning-based generative modeling for training the generative model. The first GAN architecture was described in 2014 by Ian Goodfellow in his paper titled "Generative Adversarial Networks" [72]. IoT Security can be improved by using the generative modeling architecture of GAN. The neural network systems can be trained to classify any malicious and suspicious information that might be added by hackers. Research ha shown that GAN-based security models have higher accuracy and precision, with a low rate of false-positives compared to other traditional machining learning approaches [73].

5. Research Challenges, and Future Directions

Research issues, challenges, solutions and future directions in the field of IoT security are as follows.

- Data Security and integrity:
  In machine learning techniques, reliable data for datasets and training data are very important to develop an accurate machine learning technique. A training dataset with low-quality data may interrupt the implementation of a particular learning technique. Thus, authenticated training datasets are crucial in ML techniques to secure the IoT network [74]. Furthermore, it is very easy for any hacker to learn the attack type and device vulnerabilities, and be able to manipulate the dataset used in the ML technique. Hence, it is a significant challenge to ascertain how the date can be secured and to detect different types of attacks and their probability of occurrence in any IoT environment. In other words, data security and integrity is challenging the future research field of IoT security.
- Backup Security Mechanisms:
  Usually, it is difficult to accurately state and estimate the network attack in an IoT environment in case of a "bad" defense policy in the learning process. Sometimes, this can cause disaster and drastic loss for IoT networks. Backup security mechanisms may also solve this difficulty protecting IoT systems from the exploration of the learning process. More mechanisms need to address this issue by incorporating ML-based security schemes to provide reliable, resilient and secure IoT services by reducing the risks of selecting bad policies.
- Privacy Problems:
  Privacy is a common issue in IoT environments. In IoT environments, Smart devices, such as sensors and wearable devices, are used to exchange data and information, and the users are not fully aware of where and how their personal information is shared via these devices. IoT smart devices carry the private and personal information of the clients and users, which may be misused. Every IoT device has security protocols to communicate with other devices, i.e., encryption and authentication. Privacy disclosures, leakage, and threats are crucial challenges that make users hesitate to adopt these technologies [75].
- Computational Cost:
  Many ML-based techniques require a substantial amount of training datasets and a complicated process for feature extraction, creating high computational costs and increasing the complexity of the system. Therefore, it is challenging to find new ML techniques with low communication and computational costs [76].
- Infrastructure Issues:
  A weak infrastructure always makes it easier for attackers to hack through the software. This is also known as a zero-day attack and is very difficult to determine using traditional security suits and schemes. It is, therefore, essential to build a strong and smart infrastructure to develop a secure IoT system [77]. Safety and Security features must be considered and need to be included in every phase of the IoT system.

6. Discussion

This research presented a detailed overview of the Internet of Thing (IoT) according to the latest research trends, focused on safety and security and based on machine learning techniques. To achieve this goal, recent, high-quality research papers on the subject are reviewed. The rapid advancements in the research on the security of IoT systems are supported by simulation tools and IoT modelers. Catastrophic failures in IoT networks have been observed, due to serious attacks on the security vulnerabilities in IoT devices. Due to the continuous growth in IoT devices and fewer security measures in the devices, IoT systems will remain a soft target in the future. To avoid such inconveniences, the cyber-physical security system should be considered and strong security measures should be implemented in IoT devices, such as encryption, strong authorization and authentication, and firewalls. This may be an effective means of overcoming the IoT security issues. In this research survey, the research was mainly focused on improving the lightweight encryption and authentication for resource-constrained and low-power devices.

As per the IoT security architecture presented in this paper, three layers, namely, perception/physical, network, and application layers, are considered the most recent mechanisms applied to each layer of the IoT network. It is evident that unsecured physical devices and communication networks with malicious activities result in new threats to IoT networks.

This survey also demonstrates that authentication alone may not suffice. The IoT security system needs to work on lightweight and mutual authentication systems at the application and network layers. Moreover, to mitigate physical device security issues, lightweight and low-cost encryption are proposed for the physical layer.

7. Conclusions

IoT systems have changed human life, making it easy, smooth, and comfortable. With these advancements and the development of smart things, new challenges are arising, especially those associated with the safety and security of IoT devices. The traditional methods and tools are not effective at countering the new security issues and challenges. Machine learning is a promising method, which allows for the development of various powerful methods to enhance the safety and security of IoT. In this survey, a state-of-the-art comprehensive review of the literature is presented, focusing on the safety and security of IoT, including its architecture, detailed security threats, and attack surfaces in the IoT system. In addition, a comprehensive review of the use of machine learning methods is presented. Finally, issues, research challenges, and future research directions regarding the development of a safe and secure IoT are also presented.

Author Contributions: Conceptualization, G.A., A.M. and J.L.; methodology, G.A., A.M. and J.L.; validation, M.C., G.E. and A.M.; formal analysis, A.M., M.C. and G.E.; investigation, J.L., M.C. and G.E.; resources, A.M.; data creation, G.A. and A.M.; writing the original draft: G.A. and A.M.; writing, review and editing, A.M., J.L., M.C. and G.E.; supervision, A.M., J.L. and M.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable for studies not involving humans.

Informed Consent Statement: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: All authors declare no conflict of interest.

References

1. An, P.; Singh, Y.; Selwal, A.; Singh, P.K.; Felseghi, R.A.; Raboaca, M.S. IoVT: Internet of vulnerable things? Threat architecture, attack surfaces, and vulnerabilities in Internet of Things And Its Applications Towards Smart Grids. *Energies* **2020**, *13*, 4813.
2. Airehrour, D.; Gutierrez, J.A.; Kumar, S. SecTrust -RPL: A secure trust-aware RPL routing protocol for Internet of Things. *Future Gener. Comput. Syst.* **2019**, *93*, 860–876. [CrossRef]

3. Rikli, N.E.; Alnasser, A. Lightweight trust model for the detection of concealed malicious nodes in sparse wireless ad hoc networks. *Int. J. Distrib. Sens. Netw.* **2016**, *12*, 1550147716657246. [CrossRef]
4. Yan, Z.; Zhang, P.; Vasilakos, A.V. A survey on trust management for Internet of Things. *J. Netw. Comput. Appl.* **2014**, *42*, 120–134. [CrossRef]
5. Wu, X.; Li, F. A multi-domain trust management model for supporting RFID applications of IoT. *PLoS ONE* **2017**, *12*, e0181124. [CrossRef]
6. Steinhubl, S.R.; Muse, E.D.; Topol, E.J. The emerging field of mobile health. *Sci. Transl. Med.* **2015**, *7*, 283rv3. [CrossRef]
7. Perera, C.; Zaslavsky, A.; Christen, P.; Georgakopoulos, D. Context aware computing for the Internet of Things: A survey. *IEEE Commun. Surv. Tutor.* **2013**, *16*, 414–454. [CrossRef]
8. Karlof, C.; Sastry, N.; Wagner, D.A. TinySec: A link layer security architecture for wireless sensor networks. In Proceedings of the ACM 2nd International Conference on Embedded Networked Sensor Systems, Baltimore, MD, USA, 3–5 November 2004; pp. 162–175.
9. Hussain, F.J.; Hussain, R.; Hassan, S.A.; Hossain, E. Machine learning in IoT security: Current solutions and future challenges. *IEEE Commun. Surv. Tutorials* **2020**, *22*, 1686–1721. [CrossRef]
10. Liang, F.; Hatcher, W.G.; Liao, W.; Gao, W.; Yu, W. Machine Learning for Security and the Internet of Things: The Good, the Bad, and the Ugly. *IEEE Access* **2019**, *7*, 158126–158147. [CrossRef]
11. Fadlullah, Z.M.; Tang, F.; Mao, B.; Kato, N.; Akashi, O.; Inoue, T.; Mizutani, K. State-of-the-art deep learning: Evolving machine intelligence toward tomorrow's intelligent network traffic control systems. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2432–2455. [CrossRef]
12. Modi, C.; Patel, D.R.; Borisaniya, B.; Patel, H.; Patel, A.; Rajarajan, M. A survey of intrusion detection techniques in cloud. *J. Netw. Comput. Appl.* **2013**, *36*, 42–57. [CrossRef]
13. Zhao, K.; Ge, L. A survey on the Internet of Things security. In Proceedings of the IEEE 9th International Conference on Computational Intelligence and Security (CIS), Chengdu, China, 14–15 December 2013; pp. 663–667. [CrossRef]
14. Bahtiyar, S.; Çaglayan, M.U. Extracting trust information from security system of a service. *J. Netw. Comput. Appl.* **2012**, *35*, 480–490. [CrossRef]
15. Banerjee, A.; Venkatasubramanian, K.K.; Mukherjee, T.; Gupta, S.K.S. Ensuring safety, security, and sustainability of mission-critical cyber-physical systems. *Proc. IEEE* **2012**, *100*, 283–299. [CrossRef]
16. AlTawy, R.; Youssef, A.M. Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices. *IEEE Access* **2016**, *4*, 959–979. [CrossRef]
17. Khan, Z.; Aalsalem, M.Y.; Khan, M.K. Communal acts of IoT consumers: A potential threat to security and privacy. *IEEE Trans. Consum. Electron.* **2019**, *65*, 64–72. [CrossRef]
18. Doshi, R.; Apthorpe, N.; Feamster, N. Machine learning DDoS detection for consumer Internet of Things devices. In Proceedings of the 2018 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 24–24 May 2018.
19. Abomhara, M. Cyber security and the Internet of Things:Vulnerabilities, threats, intruders and attacks. *J. Cyber Secur. Mobil.* **2015**, *4*, 65–88. [CrossRef]
20. Kolias, C.; Kambourakis, G.; Stavrou, A.; Voas, J. DDoS in the IoT: Mirai and other botnets. *Computer* **2017**, *50*, 80–84. [CrossRef]
21. Abbas, G.; Mehmood, A.; Lloret, J.; Raza, M.S.; Ibrahim, M. FIPA-based reference architecture for efficient discovery and selection of appropriate cloud service using cloud ontology. *Int. J. Commun. Syst.* **2020**, *33*, e4504. [CrossRef]
22. Subashini, S.; Kavitha, V. A survey on security issues in service delivery models of cloud computing. *J. Netw. Comput. Appl.* **2011**, *34*, 1–11. [CrossRef]
23. Bhattasali, T.; Chaki, R.; Chaki, N. Secure and trusted cloud of things. In Proceedings of the Annual IEEE India Conference (INDICON), Mumbai, India, 13–15 December 2013; pp. 1–6.
24. Faruki, P.; Bharmal, A.; Laxmi, V.; Ganmoor, V.; Gaur, M.S.; Conti, M.; Rajarajan, M. Android security: A survey of issues, malware penetration, and defenses. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 998–1022. [CrossRef]
25. Jordan, M.I.; Mitchell, T.M. Machine learning: Trends, perspectives, and prospects. *Science* **2015**, *349*, 255–260. [CrossRef]
26. Mishra, P.; Varadharajan, V.; Tupakula, U.; Pilli, E.S. A detailed investigation and analysis of using machine learning techniques for intrusion detection. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 686–728. [CrossRef]
27. Lugmayr, A.; Danelljan, M.; Timofte, R. Unsupervised learning for real-world super-resolution. In Proceedings of the 2019 IEEE/CVF International Conference on Computer Vision Workshop (ICCVW), Seoul, Korea, 27–28 October 2019; pp. 3408–3416.
28. Mnih, V.; Kavukcuoglu, K.; Silver, D.; Rusu, A.A.; Veness, J.; Bellemare, M.G.; Graves, A.; Riedmiller, M.; Fidjel, A.K.; Ostrovski, G.; et al. Human-level control through deep reinforcement learning. *Nature* **2015**, *518*, 529. [CrossRef] [PubMed]
29. Quinlan, J.R. Induction of decision trees. *Mach. Learn.* **1986**, *1*, 81–106. [CrossRef]
30. Du, W.; Zhan, Z. Building decision tree classifier on private data. In Proceedings of the IEEE International Conference Privacy Security Data Mining, Syracuse, New York, NY, USA, 14 December 2002; pp. 1–8.
31. Kotsiantis, S.B. Decision trees: A recent overview. *Artif. Intell. Rev.* **2013**, *39*, 261–283. [CrossRef]
32. Goeschel, K. Reducing false positives in intrusion detection systems using data-mining techniques utilizing support vector machines, decision trees, and Naive Bayes for off-line analysis. In Proceedings of the IEEE SoutheastCon, Norfolk, VI, USA, 30 March–3 April 2016; pp. 1–6.

33. Alharbi, S.; Rodriguez, P.; Maharaja, R.; Iyer, P.; Subaschandrabose, N.; Ye, Z. Secure the Internet of Things with challenge response authentication in fog computing. In Proceedings of the IEEE 36th International Performance Computing and Communications Conference (IPCCC), San Diego, CA, USA, 10–12 December 2017; pp. 1–2.
34. Kalaivaani, P.T.; Krishnamoorthy, R.; Reddy, A.S.; Chelladurai, A.D.D. Adaptive Multimode Decision Tree Classification Model Using Effective System Analysis in IDS for 5G and IoT Security Issues. In *Secure Communication for 5G and IoT Networks*; Springer: Cham, Switzerland, 2022; pp. 141–158.
35. Tajbakhsh, A.; Rahmati, M.; Mirzaei, A. Intrusion detection using fuzzy association rules. *Appl. Soft Comput.* **2009**, *9*, 462–469 [CrossRef]
36. Tong, S.; Koller, D. Support vector machine active learning with applications to text classification. *J. Mach. Learn. Res.* **2001**, *2*, 45–66.
37. Hu, W.; Liao, Y.; Vemuri, V.R. Robust support vector machines for anomaly detection in computer security. In Proceedings of the International Conference on Machine Learning and Applications (ICMLA), Los Angeles, CA, USA, 23–24 June 2003; pp. 168–174.
38. Liu, Y.; Pi, D. A novel kernel SVM algorithm with game theory for network intrusion detection. *KSII Trans. Internet Inf. Syst.* **2017**, *11*, 4043–4060.
39. Wagner, C.; François, J.; Engel, T. Machine learning approach for IP-flow record anomaly detection. In Proceedings of the International Conference on Research in Networking, Valencia, Spain, 9–13 May 2011; pp. 28–39.
40. Ham, H.S.; Kim, H.H.; Kim, M.S.; Choi, M.J. Linear SVM-based android malware detection for reliable IoT services. *J. Appl. Math.* **2014**, *2014*, 594501. [CrossRef]
41. Lerman, L.; Bontempi, G.; Markowitch, O. A machine learning approach against a masked AES. *J. Cryptograph. Eng.* **2015**, *5*, 123–139. [CrossRef]
42. D'Agostini, G. A multidimensional unfolding method based on Bayes' theorem. *Nucl. Instrum. Methods Phys. Res. A Accel. Spectr. Detect. Assoc. Equip.* **1995**, *362*, 487–498. [CrossRef]
43. Panda, M.; Patra, M.R. Network intrusion detection using Naive Bayes. *Int. J. Comput. Sci. Netw. Secur.* **2007**, *7*, 258–263.
44. Mukherjee, S.; Sharma, N. Intrusion detection using Naive Bayes classifier with feature reduction. *Procedia Technol.* **2012**, *4*, 119–128. [CrossRef]
45. Ng, A.Y.; Jordan, M.I. On discriminative vs. generative classifiers: A comparison of logistic regression and naive Bayes. *Adv. Neural Inf. Process. Syst.* **2002**, *14*, 841–848.
46. Ioannou, C.; Vassiliou, V. Network Attack Classification in IoT Using Support Vector Machines. *J. Sens. Actuator Netw.* **2021**, *10*, 58. [CrossRef]
47. Deng, Z.; Zhu, X.; Cheng, D.; Zong, M.; Zhang, S. Efficient kNN classification algorithm for big data. *Neurocomputing* **2016**, *195*, 143–148. [CrossRef]
48. Su, M.-Y. Real-time anomaly detection systems for denial-of-service attacks by weighted k-nearest-neighbor classifiers. *Expert Syst. Appl.* **2011**, *38*, 3492–3498. [CrossRef]
49. Li, W.; Yi, P.; Wu, Y.; Pan, L.; Li, J. A new intrusion detection system based on KNN classification algorithm in wireless sensor network. *J. Elect. Comput. Eng.* **2014**, *2014*, 8. [CrossRef]
50. Breiman, L. Random forests. *Mach. Learn.* **2001**, *45*, 5–32. [CrossRef]
51. Domb, M.; Bonchek-Dokow, E.; Leshem, G. Lightweight adaptive Random-Forest for IoT rule generation and execution. *J. Inf. Secur. Appl.* **2017**, *34*, 218–224. [CrossRef]
52. Cutler, D.R.; Edwards, T.C., Jr.; Beard, K.H.; Cutler, A.; Hess, K.T.; Gibson, J.; Lawler, J.J. Random forests for classification in ecology. *Ecology* **2007**, *88*, 2783–2792. [CrossRef] [PubMed]
53. Agrawal, R.; Imieliński, T.; Swami, A. Mining association rules between sets of items in large databases. In Proceedings of the 1993 ACM SIGMOD International Conference on Management of Data, Washington, DC, USA, 25–28 May 1993; pp. 207–216.
54. WoŸniak, M.; Graña, M.; Corchado, E. A survey of multiple classifier systems as hybrid systems. *Inf. Fusion* **2014**, *16*, 3–17. [CrossRef]
55. Zhang, C.; Ma, Y. *Ensemble Machine Learning: Methods and Applications*; Springer: New York, NY, USA, 2012.
56. Chen, Z.S.; Zhang, X.; Pedrycz, W.; Wang, X.J.; Chin, K.S.; Martínez, L. K-means clustering for the aggregation of HFLTS possibility distributions: N-two-stage algorithmic paradigm. *Knowl.-Based Syst.* **2021**, *227*, 107230. [CrossRef]
57. Hartigan, J.A.; Wong, M.A. Algorithm AS 136: A k-means clustering algorithm. *J. Roy. Stat. Soc. C (Appl. Stat.)* **1979**, *28*, 100–108. [CrossRef]
58. Jain, A.K. Data clustering: 50 years beyond k-means. *Pattern Recognit. Lett.* **2010**, *31*, 651–666. [CrossRef]
59. Münz, G.; Li, S.; Carle, G. Traffic anomaly detection using k-means clustering. In *GI/ITG Workshop MMBnet*; 2007; pp. 1–8. Available online: https://www.net.in.tum.de/projects/dfg-lupus/files/muenz07k-means.pdf (accessed on 10 June 2022).
60. Bosman, H.H.; Iacca, G.; Tejada, A.; Wörtche, H.J.; Liotta, A. Ensembles of incremental learners to detect anomalies in ad hoc sensor networks. *Ad Hoc Netw.* **2015**, *35*, 14–36. [CrossRef]
61. Wold, S.; Esbensen, K.; Geladi, P. Principal component analysis. *Chemometr. Intell. Lab. Syst.* **1987**, *2*, 37–52. [CrossRef]
62. Nobakht, M.; Sivaraman, V.; Boreli, R. A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow. In Proceedings of the IEEE 11th International Conference on Availability, Reliability and Security (ARES), Salzburg, Austria, 31 August–2 September 2016; pp. 147–156.

63. Aminanto, M.E.; Kim, K. Improving detection of Wi-Fi impersonation by fully unsupervised deep learning. In *International Workshop on Information Security Applications (WISA)*; Springer: Cham, Switzerland, 2017; pp. 212–223.
64. Shi, C.; Liu, J.; Liu, H.; Chen, Y. Smart user authentication through actuation of daily activities leveraging WiFi-enabled IoT. In Proceedings of the 18th ACM International Symposium on Mobile Ad Hoc Networking and Computing, Chennai, India, 10–14 July 2017; p. 5.
65. Meidan, Y.; Bohadana, M.; Shabtai, A.; Guarnizo, J.D.; Ochoa, M.; Tippenhauer, N.O.; Elovici, Y. ProfilIoT: A machine learning approach for IoT device identification based on network traffic analysis. In Proceedings of the ACM Symposium on Applied Computing, Marrakech, Morocco, 3–7 April 2017; pp. 506–509.
66. Lakhotia, A.; Kapoor, A.; Kumar, E. Are metamorphic viruses really invincible. *Virus Bull.* **2004**, *12*, 57.
67. Miettinen, M.; Marchal, S.; Hafeez, I.; Asokan, N.; Sadeghi, A.-R.; Tarkoma, S. IoT sentinel: Automated device-type identification for security enforcement in IoT. In Proceedings of the IEEE 37th International Conference on Distributed Computing Systems (ICDCS),Atlanta, GA, USA, 5–8 June 2017; pp. 2177–2184.
68. Smys, S.; Basar, A.; Wang, H. Hybrid intrusion detection system for internet of things (IoT). *J. ISMAC* **2020**, *2*, 190–199. [CrossRef]
69. Li, Q.; Zhang, K.; Cheffena, M.; Shen, X. Channel-based sybil detection in industrial wireless sensor networks: A multi-kernel approach. In Proceedings of the IEEE Global Communications Conference (GLOBECOM), Singapore, 4–8 December 2017; pp. 1–6.
70. Rathore, S.; Park, J.H. Semi-supervised learning based distributed attack detection framework for IoT. *Appl. Soft Comput.* **2018**, *72*, 79–89. [CrossRef]
71. Niknam, S.; Dhillon, H.S.; Reed, J.H. Federated learning for wireless communications: Motivation, opportunities and challenges. *arXiv* **2019**, arXiv:1908.06847.
72. Brownlee, J. A gentle introduction to generative adversarial networks (GANS). *Tutor. Gan Lin395c Res. Comput. Linguist.* **2019**, *17*.
73. Ferdowsi, A.; Saad, W. Generative adversarial networks for distributed intrusion detection in the internet of things. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019.
74. Musonda, C.; Monica, M.K.; Nyirenda, M.; Phiri, J. Security, Privacy and Integrity in Internet of Things—A Review. In Proceedings of the ICTSZ International Conference in ICTs, Lusaka, Zambia, 18 July 2019; pp. 148–152.
75. Ferrag, M.A.; Shu, L. The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: A tutorial. *IEEE Internet Things J.* **2021**, *8*, 17236–17260. [CrossRef]
76. Ferrag, M.A.; Shu, L.; Friha, O.; Yang, X. Cyber Security Intrusion Detection for Agriculture 4.0: Machine Learning-Based Solutions, Datasets, and Future Directions. *IEEE/CAA J. Autom. Sin.* **2021**, *9*, 407–436. [CrossRef]
77. Hussain, M.; Mehmood, A.; Khan, S.; Khan, M.A.; Iqbal, Z. Authentication techniques and methodologies used in wireless body area networks. *J. Syst. Archit.* **2019**, *101*, 101655. [CrossRef]