electronics

MDPI

Article

MADS Based on DL Techniques on the Internet of Things (IoT): Survey

Hussah Talal [1,*] and Rachid Zagrouba [2]

[1] Department of Computer Science, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 7059, Dammam 32252, Saudi Arabia
[2] College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia; rmzagrouba@iau.edu.sa
* Correspondence: Hussah_Talal@outlook.sa

Abstract: Technologically speaking, humanity lives in an age of evolution, prosperity, and great development, as a new generation of the Internet has emerged; it is the Internet of Things (IoT) which controls all aspects of lives, from the different devices of the home to the large industries. Despite the tremendous benefits offered by IoT, still there are some challenges regarding privacy and information security. The traditional techniques used in Malware Anomaly Detection Systems (MADS) could not give us as robust protection as we need in IoT environments. Therefore, it needed to be replaced with Deep Learning (DL) techniques to improve the MADS and provide the intelligence solutions to protect against malware, attacks, and intrusions, in order to preserve the privacy of users and increase their confidence in and dependence on IoT systems. This research presents a comprehensive study on security solutions in IoT applications, Intrusion Detection Systems (IDS), Malware Detection Systems (MDS), and the role of artificial intelligent (AI) in improving security in IoT.

Keywords: anomaly detection system; machine learning techniques; Deep Learning (DL) techniques; IoT devices; IoT networks; malware detection

Citation: Talal, H.; Zagrouba, R. MADS Based on DL Techniques on the Internet of Things (IoT): Survey. *Electronics* **2021**, *10*, 2598. https://doi.org/10.3390/electronics10212598

Academic Editors: Hamed Taherdoost, Seyed Reza Shahamiri, Kamaljeet Sandhu, Basit Qureshi, Hazra Imran and Salimur Choudhury

Received: 18 September 2021
Accepted: 12 October 2021
Published: 24 October 2021

1. Introduction

We live in the age of evolution, technical progress, and transformation into a new fantasy world. It is the world of the Internet of Things (IoT). Everything in the IoT world is connected to other things in a very intricate manner to the extent that they cooperate, exchange information, and move to serve human beings without the need for any major efforts on the part of humans.

In fact, the world of IoT provides many different services and endless opportunities to human beings as it is mainly concerned with the small and minute details of human life and the daily interactions and transactions. Moreover, when somebody wakes up, the intelligent air conditioning, for example, would reset the room's temperature based on the temperature of his body. In fact, IoT systems are used in many areas such as in the industry, commerce, smart cities, and other sectors. The number of devices that will be connected to the Internet by 2025 is expected to reach 75.44 billion devices up from 15.41 billion in 2015 [1]. This means an increase of 489.6%.

However, with the remarkable increase in the numbers of devices that are being connected to the Internet, the concerns about security and privacy issues have increased. Any penetration into one IoT device may cause a violation of the entire IoT network. Usually, IoT devices have simple resources and limited power consumption, therefore, it is difficult to use complex security protocols on them. For these reasons, scientists have recently become more and more interested in conducting and doing research to improve security and maintain privacy in IoT environments.

One of the most effective solutions to increase security in IoT environments is using Intrusion Detection Systems (IDS). In fact, IDS are appropriate to avoid attacks or attempts

of penetration before they happen and harm the IoT system and its users, as it can predict unexpected attacks then alert the user. The Intrusion Prevention System (IPS) does the same work as IDS but with in addition to that, it can stop the attacks just before they happen [2].

Kaspersky published on their website [3] the statistics on IoT attacks after analyzing the Kaspersky honeypots. They stated that in the first half of 2019, the number of attacks reached 105 million attacks on IoT devices coming from 276,000 unique Internet Protocol (IP) addresses, which means that the number of attacks has increased seven times compared to 2018, when there were 12 million attacks from 69,000 IP addresses. Cybercriminals are intensifying their attacks on IoT due to the poor security in IoT products to create IoT botnets. Based on the results of analysis data obtained from Kaspersky honeypots, they found out that the attacks were not complicated, and that the user might not notice that his device was exploited by a cybercriminal, as if the latter is a ghost. According to Kaspersky's statistics, 39% of the attacks were from the malware family [3], hence the importance of developing Malware Detection Systems (MDS), to discover the malware and prevent it from causing any damage to the IoT system.

The importance of using Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) techniques to build MDS, which is appropriate to IoT environments, has appeared to increase the effectiveness of MDS and improve their predictability in the IoT environment, according to the nature of the IoT which is connecting all things with one another permanently and to the Internet. In spite of the amount of research and development that scientists and professionals have put into the security of IoT environments, there are still some vulnerabilities and defects on it. As a result of the increase in the number of malwares as well as the emergence of intelligent malwares which constantly renew themselves, there is a need to build an MDS that has a very high ability to detect both known and unknown malwares, and that also has a high accuracy, in order to obtain an intelligent security system in IoT environments.

This paper aims to help researchers know the achievements and contributions of scientists and researchers in the field of developing and improving security in IoT environments and overcoming malware attacks. It presents a comprehensive study, including the security solution in IoT applications, studies related to ML-based security solutions in IoT, studies related to IDS-based security solutions in IoT, ML-based IDS, ML-based IDS for IoT security, studies related to DL-based IDS for IoT security, and papers related to DL-based MDS for IoT security. Then, it discusses the challenges in the field of using MDS in IoT environments. Finally, it presents the analysis, findings and conclusion.

2. Background

2.1. IoT

This section presents the IoT definitions, architectures, threats, and malware taxonomy in IoT.

2.1.1. IoT Definitions

Scientist defined the IoT term in different ways according to their interests. The IoT definitions have emerged from several organizations or entities that are working in the field of communications and technology. Some of them focus on the infrastructure of the IoT, others focus on the way of communicating between devices, and some others focus on the connection of these devices to the Internet. We mention, below, some of these definitions:

IBM [4] defined IoT as a huge network that connects humans and things and smart things with each other. It connects any device to any other device or to the Internet, each device providing information about its environment while also collecting and sharing data about how they interact with their environment.

Oracle [5] defined IoT in the following manner: "by means of low-cost computing, the cloud, big data analytics, and mobile technologies, physical things can share and collect data with minimal human intervention. In this hyperconnected world, digital systems can

record, monitor, and adjust each interaction between connected things. The physical world meets the digital world—and they cooperate".

With respect to the previous definitions, in our perspective, we define IoT as everything connects to everything and connects to the Internet in an intelligent way, converting everything to be smart and interactive.

2.1.2. IoT Architectures

IoT has many different architectures for different IoT applications. The IoT architectures are independent of each other. Some are designed to present communication between devices, while others focus on the devices' connection to the Internet through the gateway. However, these architectures still lack security, privacy, and scalability. Up to now, the IoT area lacks unified architecture. Therefore, there is a need to design a unified architecture for IoT and its various applications [6,7]. Figure 1 presents a comparison between 3, 4, and 5 layers of IoT architectures. In the following sections, we mention some of these architectures:

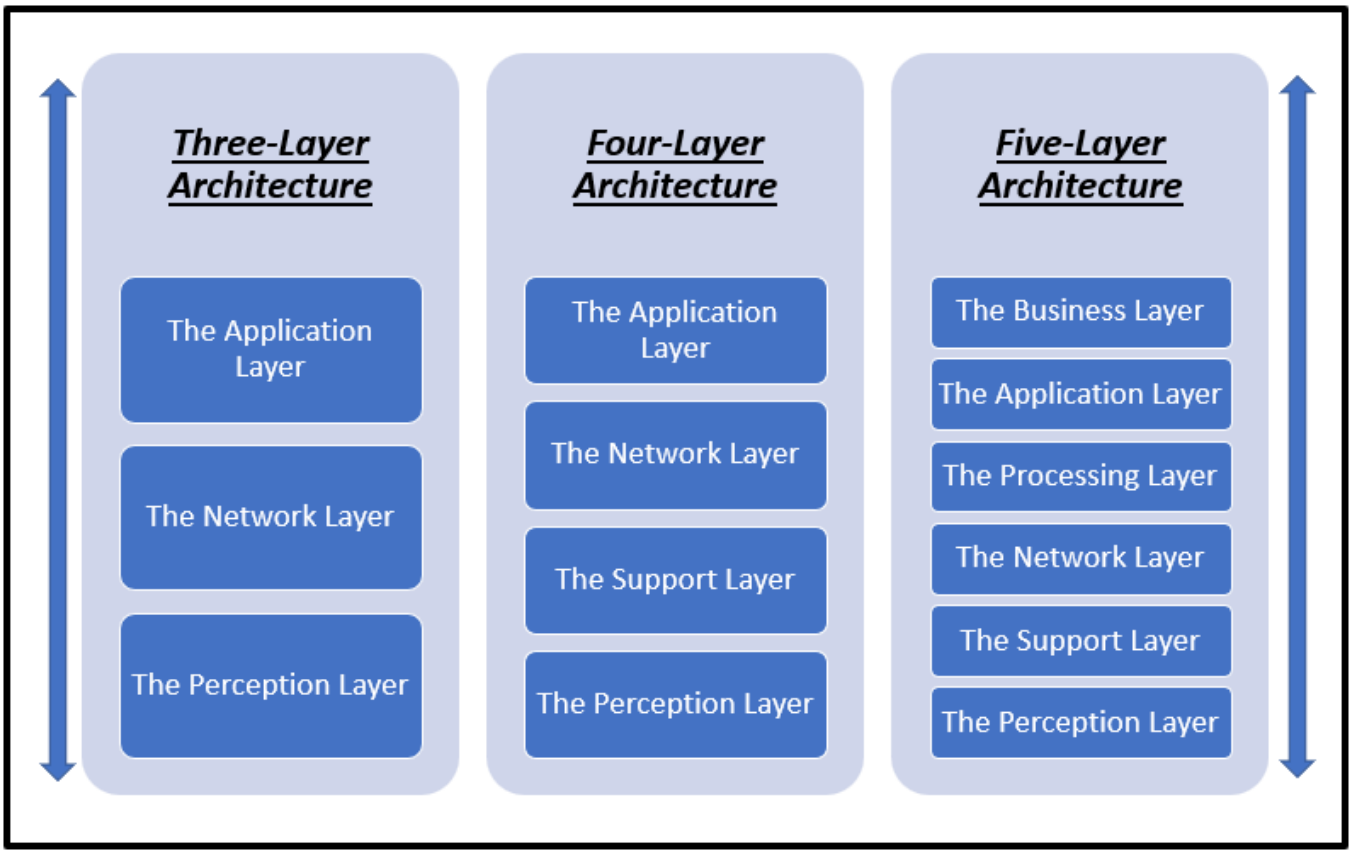

Figure 1. Comparison between 3, 4, and 5 layers of IoT architectures.

(1) Three-Layer Architecture

This is the simplest IoT architecture, which contains the basic IoT layers, and is considered the basic IoT architecture that was developed in the beginning of IoT. It consists of three layers [6,8]:

- The Perception Layer

This is also called the sensors layer. It contains sensors that interact with the external environment and collect data from it. It works like the human sensory system because it sees, hears, and feels. The sensors differ according to the IoT applications and its purpose. This layer is exposed to a variety of attacks such as eavesdropping, fake node and malicious timing attack, and replay attack [6].

- The Network Layer

The network layer is responsible for the connection between smart objects, services, and network devices. It also transfers collected data using sensors from the sensor layer to the application layer. Some researchers call it the transport layer.

It is considered one of the most vulnerable layers for attacks and attackers. Up to now, researchers have concerns about the data authentication and integrity in this layer. Some of the attacks that occur to this layer are Denial of Service (DoS) attacks, storage attacks, Main-In-The-Middle (MITM) attack, and exploit attacks [6].

- The Application Layer

The application layer is responsible for providing services to the end-user; the services differ according to the IoT applications and data gathered from the sensors.

The application layer has many issues, including security issues, as well as issues related to some applications of IoT, such as power and storage. Some potential attacks to this layer are malicious code attack, cross site scripting, and dealing with a huge amount of data [6].

(2) Four-Layer Architecture

With the progress and development in the IoT field, some researchers have proposed an amendment to the three-layer architecture by adding a new layer, the support layer, which is responsible for security issues.

Three layers of the four-layer architecture have similar functionality to the layers in three-layer architectures, which are the perception layer, application layer, and network layer that were explained previously. The fourth layer of the four-layer architecture is the support layer [6].

- The Support Layer

This is a layer responsible for security issues and has two basic responsibilities. The first responsibility is to verify the sender and check the integrity of the information, and the second is to send information to the network layer. This layer has been exposed to some attacks, such as the malicious insider attack and DoS attack [6].

(3) Five-Layer Architecture

The researchers discovered that the four-layer architecture was facing some security problems, so some researchers suggested the five-layer architecture by enhancing the three-layer architecture with two additional layers for IoT security. These two layers are [6,8]:

- Processing Layer

This is responsible for collecting data, extracting useful information from it, and removing noise and unhelpful data. It improves big data functionality and is also called the middleware layer. It faces some attacks such as malwares and exhaustion [6].

- Business Layer

This has the role of controlling and managing IoT applications, is concerned with user privacy, and takes the administrator role for the whole system. Some examples of attacks that may face the system are zero-day attack and business logic attack [6].

(4) Social IoT (S-IoT) Architecture

In S-IoT architecture, smart devices and services are dealt with in the same way as humans do in their social relationships, allowing acquaintance and getting trust between devices. The main goal in IoT architecture is to transfer the principle of social networks to the IoT. It is similar to a three-layer architecture; it consists of a sensing layer, a network layer, and an application layer. The application layer is considered as the middleware layer [8,9].

(5) Cloud- and Fog-Based Architectures

In some architectures, the emphasis was placed on protocols, but dealing with data was ambiguous. Cloud- and fog-based architectures are very interested in data, its processing, and its storage. In cloud-based architecture, they centralized the cloud with all devices connected to it, and the IoT network is at the bottom, where most of the data-related work, such as storing, processing, and using AI are done on the cloud.

Recently, a new architecture has been suggested, which is fog-based architecture. In fog computing, both gateways and sensors bear a portion of the workload and data processing. The developer modified the five-layer architecture by adding four new layers between the transport layers and the sensors layer. These layers are the monitoring layer, pre-processing layer, storage layer, and security layer, where the tasks are distributed between these layers. This architecture is for both cloud and fog.

One of the main advantages of this architecture is the improved performance of real-time systems, security, and efficiency, as well as the resource consumption and bandwidth between the cloud and the gateway [8,10].

2.1.3. IoT Threats

IoT threats are divided into two sections: natural threats and human threats. The natural threats occur due to natural causes, such as earthquakes, floods, and fires. Human threats are often in the form of malicious attacks, such as guessing passwords or using malicious spyware [11].

With the increased dependence on IoT in different aspects of life and the need to get connected to the Internet permanently, a concern has developed about privacy and security. IoT devices often have low energy and lower computing resources ability. Therefore, it is difficult to use complex security protocols on them and this is considered a vulnerability in IoT devices in terms of security; penetrating one device can lead to the penetration of the entire IoT network. The common vulnerabilities in IoT device are weak passwords, lack of encryption, backdoors, and Internet exposure [11,12].

Malware is sent to IoT smart devices with the aim of tampering, sabotaging, spying, and stealing information, as well as many other targets. Examples of malware attacks, which an attacker often makes in groups to become stronger, are DoS attacks, spam bots, brickers, and cryptomining bots. There are also some examples of recent IoT malware: TimpDoor, DeepLocker, and spam bots. Classic IoT Malware attacks, old but created a great revolution and are the basis for most new versions of malware, include Mirai and Brickerbot [12].

2.1.4. Malware Types

The following paragraphs present the most popular types of malware [1,2,13,14], as shown in Figure 2.

Figure 2. Malware types.

- Virus

This is a type of malware that was very common previously, but with the development of protection programs, they have decreased significantly in the present time. They infect specific files or software and start working when opening or executing files or programs. Usually, they can repeat themselves and infect other files. They are confidential and ambiguous.

- Adware

This is a type of malware which is specialized in showing unwanted ads, such as ads that appear in pop-up windows, or redirecting the browser to an ads page. Some advertising companies often develop this type of malware to promote their ads. Some of them are specified for advertising only, which is considered the lightest harm to the system, but others may contain further malicious software for spying or damaging the system.

- Spyware

A type of malicious program that spies on the user and monitors his movements. The goals of this type of malware vary depending on the source's target. It may come with an adware. Not all spyware malicious programs are considered harmful, but they always violate privacy.

- Worms

This is a malicious software that is similar to the virus's behavior. The main difference between them is that the worm does not need a program or file to execute itself, where it can largely repeat itself, transmits between devices, and causes damage and destruction to different files.

- Trojan horse

This is one of the most dangerous types of malware, it is formed as a legitimate or anti-virus program, but it contains malicious instructions that collect financial and private data. It is considered the weapon of choice for hackers and it is often used to install ransomware and keyloggers software.

- Ransomware

This is a modern type of malware which encrypts important data and asks for ransom in order to decrypt them. Most attacks are caused via Trojan files. In order to ensure data protection, it is preferable to keep a backup of important data for retrieval in the event of exposure to this type of malware.

- Rootkit

This is a malicious software that gives unauthorized users a full authority to control the system and its various components. In case a computer gets infected by such type of virus, experts recommend that you wipe the entire hard drive and reinstall everything.

2.2. MDS

This section presents the definition, types, and techniques of MDS. Moreover, it presents a comparison between IDS and firewalls.

2.2.1. MDS Definition

Malware is a type of intrusion. Thus, MDS is an automated system that performs the process of analyzing, monitoring, researching, and continuing exploration to identify any strange or suspicious movement within the network or between networks, whether it is a malicious software, a violation of policies, a change in the powers and authority granted to a user, encryption of the data, or a theft of data. Then, MDS sends alerts to the system administrator when something suspicious is detected [15–17]. Figure 3 presents the MDS in IoT environments.

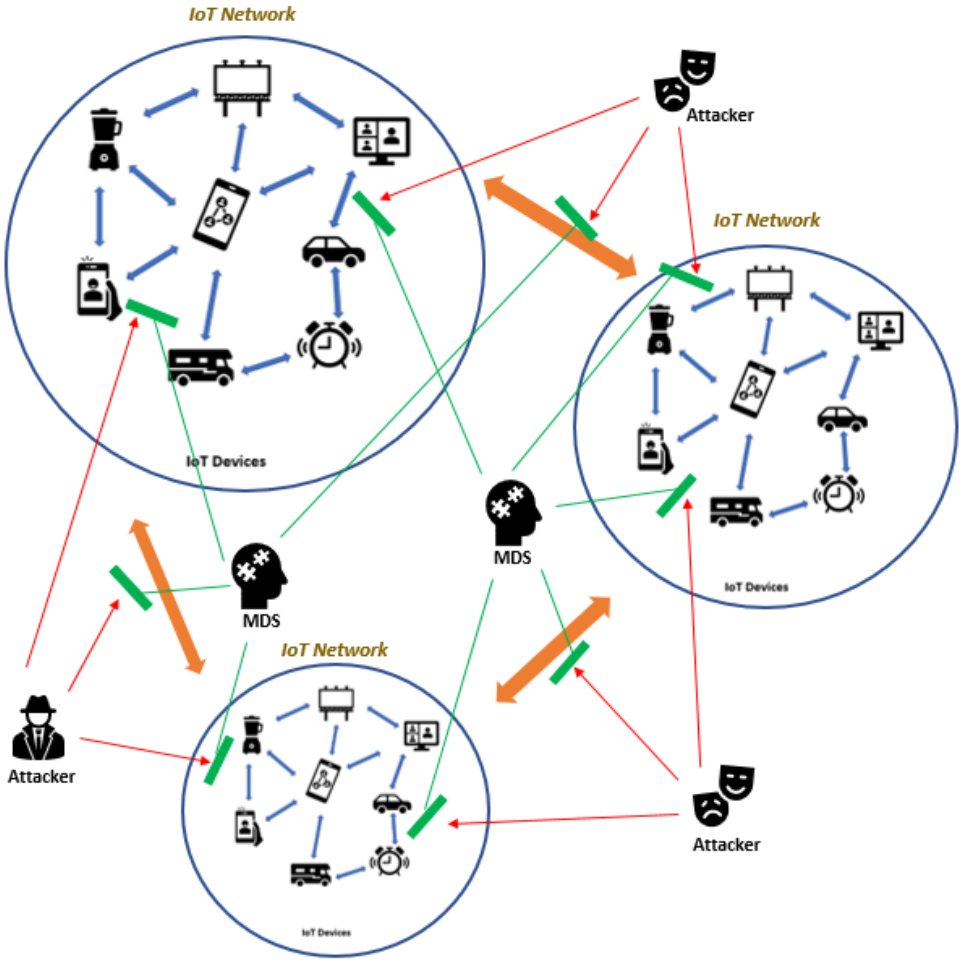

Figure 3. MDS in IoT systems.

2.2.2. MDS Types

MDS are made up of two main parts: network-based MDS and host-based MDS. Below is the explanation of each type.

- Network-Based MDS

Network-based MDS focus on protecting networks from harmful attacks and monitoring network traffic to protect network assets from malware. Network-based MDS have two types: wireless MDS and the Network Behavior Analysis (NBA) MDS. The first type, as the name implies, monitors wireless networks. The second type monitors network traffic to explore any suspicious movement or intruders [16,18].

- Host-Based MDS

This type works on information assets, whether they are servers or hosts. It is installed on one asset, monitors its activity, and protects it from malware and suspicious movements. It is known as an integrity verifier system [16]. Within this category, the following type stands out:

- The HMDS-Based Application

This type protects a single application on one or more hosts and protects this application from specific types of attacks [16,18].

2.2.3. MDS Techniques

The techniques of MDS used for monitoring network traffic or hosts are divided into three main sections: signature-based MDS, anomaly-based MDS, and stateful protocol analysis [15,16,18].

- Signature-Based MDS

Signature-based MDS detects attacks have certain patterns and distinctive signatures stored in its database. By comparing every signature entered to a system with the signatures that are stored within it, when entered signatures match with the stored signatures of the malware, MDS will prevent it from entering the system. The disadvantage of this system is that it could not reveal the new signatures of the attackers and malicious software [15,16,18].

- Anomaly-Based MDS

This system is distinguished by its ability to detect known and unknown malicious attacks. It is trained to understand the surrounding environment and natural movement. After that, it gets the ability to distinguish and identify any strange movements or suspicious attacks. AI, ML, and DL are often used in MDS to improve the predictability and detection of the new types of attacks [15,16,18,19].

- Stateful Protocol Analysis

This type analyzes network traffic by tracking internal and external network connections and recording all movements and connections in records. Then, it compares the profiles of benign protocols known to the records that the system monitored. This reflects the concept of a signature-based system [15,16].

Usually, more than one type of detection system is integrated to obtain highly accurate and effective systems. Figure 4 presents the taxonomy of MDS types and techniques.

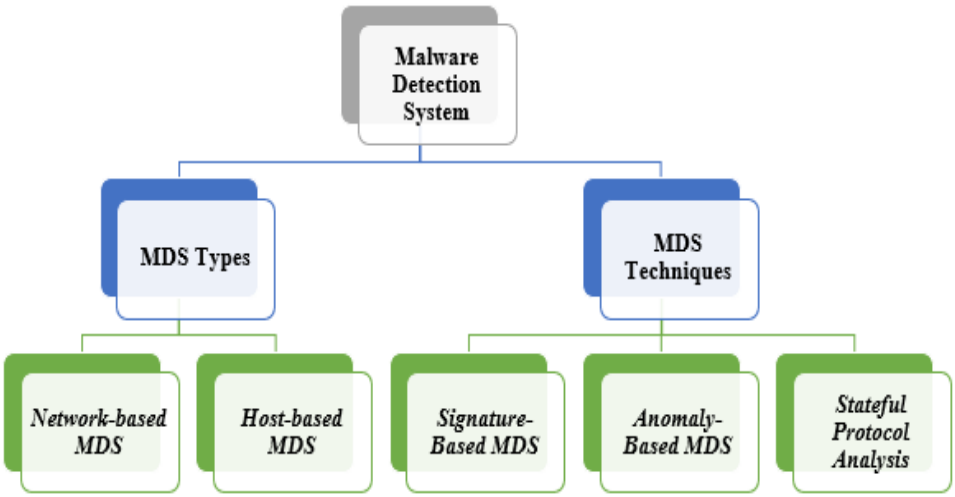

Figure 4. MDS types and techniques.

2.2.4. Comparing IDS with Firewall

Both IDS and firewalls are responsible for network security. Firewalls intercept visible breaches to prevent them from occurring. They also prevent attacks across networks, but they cannot recognize the internal attacks.

IDS prevent attacks and intrusions inside the network, as well as prevent attacks across networks, and in case the attack is suspected, it makes an alert to the system administrators to take the appropriate action. The IDS prevents attacks from reaching applications such as a firewall [20].

3. Security Solutions in IoT Applications

This section discusses the security solutions for smart cities, smart homes, and oil and gas, as shown in Figure 5.

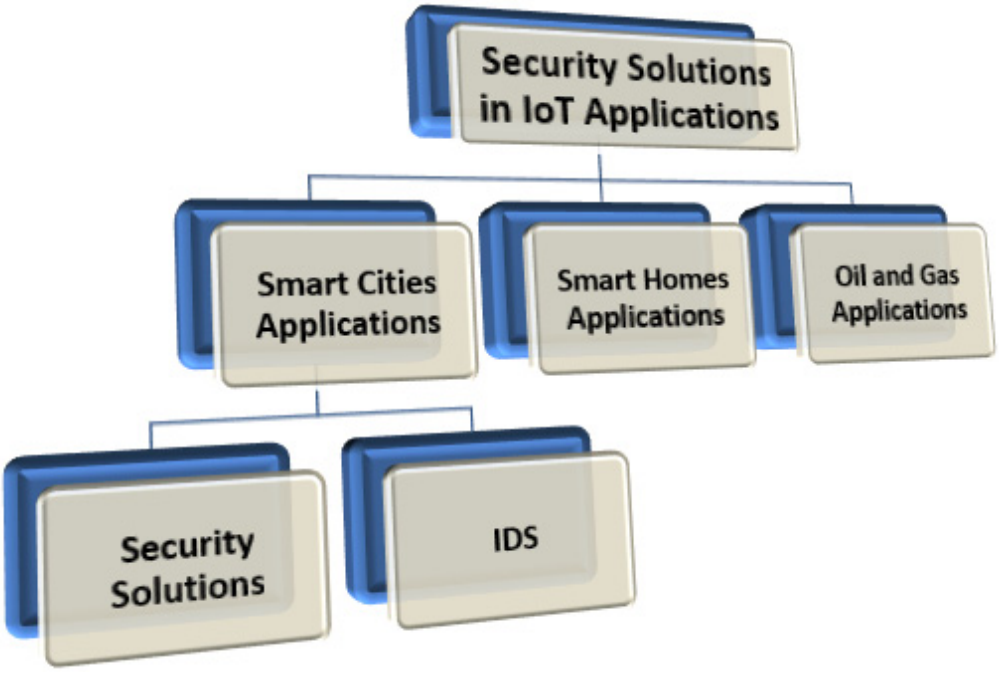

Figure 5. Security solutions in IoT applications.

3.1. Smart Cities Applications

This section discusses the security solutions and IDS in IoT-based smart cities.

3.1.1. Security Solutions in IoT-Based Smart Cities

One of the most important applications of IoT is smart cities. They have a great importance in developing, facilitating, and solving many problems and challenges in humans' lives. Scientists and researchers have made great efforts related to this field. In the following, we will mention some scientists and researchers' efforts.

Smart cities have become the focus of attention for many developers, planners, businessmen, and scientists. This is because of their great benefit in improving livelihoods and conserving resources. As a result of the nature of smart cities and the many devices connected to each other, the hackers know that the infrastructures of smart cities are vulnerable to penetration. Therefore, scientists and researchers in this field are interested in developing systems of protection and the preservation of privacy. The protection of a smart city relies on four main concepts [21]:

i. Management of the access system.
ii. Prevention of different kinds of threats.
iii. Discovery of different devices and identification of their ID.
iv. Preservation of the integrity of data.

Din, M. Guizani et al. discussed in [22] different ML techniques which are expected to play an important role in the development of security systems in IoT. In [23], they discussed different limitations and challenges in IoT-based smart cities. They also discussed the proposed solutions. There are four important elements that play essential roles in the smart city system, these smart elements are:

i. Citizens.
ii. Things.
iii. Spaces.
iv. Systems.

In [24], the authors carried out a comprehensive study of the various challenges and threats in smart cities, then they analyzed vulnerabilities and identified potential threats. The authors identified four main elements that are threatened:

i. Smart vehicles.
ii. Smart grids.
iii. Unmanned aerial vehicles.
iv. Building automation systems.

They also discussed in detail and analyzed the forensic investigations in smart cities. Authors in [25] discussed the IoT-based smart city and the threats in different layers. They discussed the solution of threats to improve security systems in IoT-based smart cities.

In [26], the researchers discussed the SMARTIE project and its benefits in smart city applications. They discussed internal and external threats. They presented different uses and cases for applied SMARTIE projects in different IoT stations. In [27], the authors proposed a new framework to improve security in future smart cities called SEFSCITY. Their framework depended on distributed computing and IoT cloud computing. The architecture of their framework depended on the cloud federation technique and multi-cloud. After that, they proposed a security protocol to secure their proposed framework. The new security protocol used Zero-Knowledge Proofs (ZKP), depending on the Elliptic Curve Discrete Logarithm Problem (ECDLP). Finally, they created many scenarios to evaluate their framework. They implemented their experiment by the cloud analyst tool. The results for all scenarios showed that the cost of infrastructure is beneficial to the cloud provider only, but it remains the same for the cloud client. This proposal is useful for the cloud provider in terms of data processing time and revenue. In [28], the authors proposed a new framework for a smart home. Their IoT security frameworks were composed of four layers:

i. Application.
ii. Network.
iii. Devices.
iv. Services.

They analyzed the attacks in each layer. Then, they presented the procedure to develop a model for a general threat to determine the vulnerabilities and the possible countermeasures in each layer to reduce the risk and improved security. After that, they proposed a new approach to detect anomalies in the first layer called ABA-IDS. The result of their evaluation presented the effectiveness of using this approach in each layer for normal procedures. It is also effective in known and unknown attacks detection in IoT devices. The false alarm became low and the rate of detection became high.

In [29], the authors presented an overview of the main concepts of smart city architecture. They reviewed the last projects for smart cities and initiatives. They highlighted the vulnerabilities and issues of privacy in smart cities that need to be processed. Finally, they discussed the different solutions related to privacy and security, standards, recommendations, and services in smart cities.

In [30], the authors studied the current state of security and privacy in smart cities. Then, they presented their insight into smart cities and discussed security and privacy issues in the smart applications of the IoT. They discussed the prerequisites for building a smart, safe, and stable city. After that, they summarized the current protection methods. Finally, they presented open challenges in this field to overcome them and develop them in the future.

Table 1 presents a comparison between the related studies [28,31–33] based on many parameters, proposed solutions, techniques, detection approaches, dataset, accuracy, complexity, scalability, and results, in order to discuss the related works of the security system in IoT-based smart cities.

Table 1. Security system in IoT-based smart cities.

Ref.	Proposed Solutions	Techniques	Detection Approaches	Dataset	Accuracy	Complexity	Scalability	Result
[28]	A new framework for a smart home security and its vulnerabilities.	-Sensor-DNA-profile (s-DNA)	Anomaly	-	-98% for known attacks -Up to 95% for unknown attacks	They proposed a complex framework consisting of four layers: devices, network, services, and application.	-	-The false alarm became low. -The rate of detection became high.
[31]	Detection of anomalies in loT- based smart city using the Random Forest ML algorithm (AD-IoT). Distributed on the fog network.	Random Forest ML algorithm	Anomaly	UNSW-NB15	99.34%	It is a complex system because it consists of massive of devices, cloud, and fog network which interact together. It also analyses the traffic between them.	The system is scalable due to its dependence on fog network and cloud.	They prove the effectiveness of their proposed model. The false positive rate is low and the accuracy is high.
[32]	Proposed new face recognition to improve the security system in IoT environments.	-Raspberry pi (RPI) -Global system for mobile communication (GSM) -Local area network (LAN) -Universal Serial Bus (USB) -Wi-Fi router -SIM card	-	Known persons in database.	-	-	-	This proposal is effective and can be used in different sectors.
[33]	They proposed a new framework for an IDS and schema for classification attacks.	WSNs	-Rule-based detection -OC-SVM	WSN attacks	-	They reduced the complexity of the security administration using SIEM technology.	Adding SIEM technology to their proposed framework guarantees scalability.	The aim of their proposal is helping the administrators of a smart city to determine the most attacks, components, and service providers affected by the attacks.

Table 2. IDS in IoT-based smart cities.

Ref.	Proposed Solutions	Techniques	Detection Approaches	Dataset	Accuracy	Result
[34]	The authors proposed an automated secure framework for a continuous availability of cloud service for connected vehicles.	- DT - DBN	Anomaly	- NS-3 simulator for normal networks behavior - NSL-KDD for intrusion behavior	99.43%	The result of their experiment evaluation proved the effectiveness of the IDS and they got 1.53% for the rate of false negatives, 0.96% for the rate of false positives, and 99.92% for the rate of detection.
[35]	They proposed a new framework for an IDS to detect the DDoS attacks in the network of smart cities.	- RBMs - FFNNs - K-means clustering algorithm	Anomaly	Dataset collected from the smart water distribution system in a smart city	Layer 1 = 97.5 Layer 2 = 97.12 Layer 3 = 96.72	The result of the evaluation of experience proved that this framework is effective and efficient in smart cities networks to detect DDoS attacks.

3.1.2. IDS in IoT-Based Smart Cities

M. Aloqaily et al. proposed in [34] an automated secure framework for continuous availability of a cloud service for connected vehicles, based on an improved IDS technique to protect the environment from cyber-attacks and achieve users' Quality of Experience (QoE) and Quality of Service (QoS) demands. Their contributions in their paper were as follows.

The node of the vehicle assembly technique adapted to ensure communication with providers of service is only done between group heads, the entities of trusted third-party providers of service. The authors proposed an IDS and evaluated it in three stages. This mechanism is integrated for trusted third parties, group heads, and the providers of service. They also proposed a framework for an IDS that combines two techniques: Decision Tree (DT) to reduce data dimension and Deep Belief Network (DBN) for surveillance. They called their framework D2H-IDS. The result of their experiment evaluation proved the effectiveness of the IDS and they got 1.53% for the rate of false negatives, 0.96% for the rate of false positives, an accuracy of 99.43%, and a rate of detection of 99.92%. In [35], the authors proposed a new framework for an IDS to detect the Distributed Denial of Service (DDoS) attacks in the network of smart cities. In their proposal, they used it to extract the features from row data that are collected from the smart environment: the Restricted Boltzmann Machines (RBMs) which use unsupervised methods to deal with row data and extract the features. Then, for training the model, they used a classification technique; Feed-Forward Neural Networks (FFNNs). They used it to evaluate their model dataset collected from the smart water distribution system in a smart city. The result of the evaluation of experience proved that this framework is effective and efficient in smart cities networks to detect DDoS attacks.

Table 2 presents another comparison based on many parameters, which are proposed solutions, techniques, detection approaches, dataset, accuracy, and result, in order to discuss the related works of IDS in IoT-based smart cities.

3.2. Smart Home Applications

A smart home is one of the IoT applications: all smart home devices are connected to the Internet through a basic unit. The user can control various home devices through an application that the user downloads on a smartphone. Smart homes also contribute to saving energy, reducing electricity consumption, and enhancing safety. The user can monitor his home from anywhere around the world. In case there is any attempt to enter the home from intruders, the smart home blocks the intruders and informs the homeowner to take the appropriate action. Smart homes also provide useful services, including the ability to detect and stop gas leaks and inform the user about this imbalance, which contributes to overall safety from fires and protecting the elderly and children. Smart homes provide a safe and comfortable life for humans [36]. Authors in paper [37] proposed a classification model based on the logistic regression method. They collected their data from 41 IoT devices. The accuracy was 99.79%. Their model is appropriate for a dynamic and heterogeneous environment, such as a smart home.

3.3. Oil and Gas Applications

One of the most important IoT applications is IoT-based oil and gas. IoT has a major role in increasing productivity and efficiency in oil and gas fields through monitoring pressure and temperature, as well as detecting leaks and making predictions of any potential dangers. It contributes to avoiding dangers and helps in detecting if there is any theft or tampering in the oil or gas field. Scientists and researchers have developed various technologies and suggested systems to monitor and protect against attacks, intruders, and risks, that could contribute to developing and improving the efficiency and effectiveness of using IoT in oil and gas field [38–46].

IoT is involved in many different aspects of life and contributes in developing them and overcoming most of their problems and challenges in smart ways, such as the use of

IoT systems in the industry, commerce, healthcare, education, agriculture, and traffic, and weather predictions.

4. Security Solutions

This section presents the studies related to security solutions in IoT and other environments. Figure 6 present the approach taken to analyze the studies in this paper.

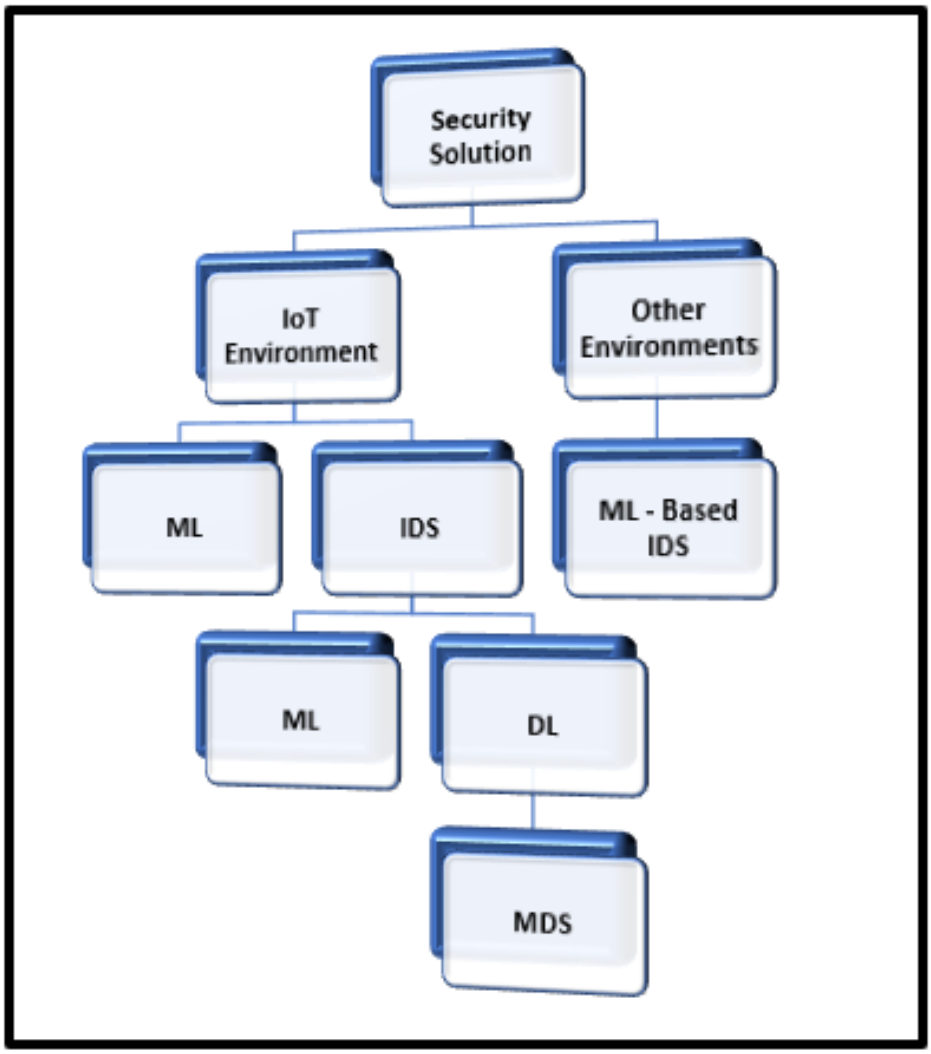

Figure 6. The structure of the paper.

4.1. Security Solutions in IoT

This section presents the studies related to the security solutions in IoT based on ML and DL.

4.1.1. ML-Based Security Solutions in IoT

Scientists and researchers have made great efforts to increase security and maintain the privacy of users in IoT environments to obtain an intelligent and safe environment for humans. Below, we mention some of the scientists' efforts in ML techniques for IoT environments' improved security and IDS. In paper [47], the authors proposed a new framework depending on ML for different characterizations of network traffic, to determine and classify the baseline behavior for different devices in the IoT network. They presented in their paper four contributions:

i. They simulated a smart environment using 28 IoT devices in the living lab. Their IoT devices included motion sensors, plugs, cameras, lights, and appliances. They collected and processed their data for six months, then they made a subset of their collected data available to the public.
ii. They recognized the main statistical features, for example, signalling patterns, cipher suites, activity cycles, and port numbers. Then, they used them to get the overview of the main features of network traffic.
iii. They developed a new ML algorithm with a multi-step for classification and determined the identity of each IoT device. They got 99% accuracy depending on the behavior of the network.
iv. They evaluated their framework by testing the balance between the accuracy of the classifier, costs, and speed.

They proved, in their paper, depending on the network behavior analysis, that each IoT device connected to the network could accurately be identified. In [48], the authors proposed a new lightweight approach to detect DDoS malware in the environment of IoT. They extracted the image of malware then they used a convolutional neural network technique to classify their category. After evaluating the results of their experiment, they proved the effectiveness of the proposed approach and that the approach could be modified to be more effective by using different techniques to reduce the size of the network. The authors in [49] said that the use of traditional authentication techniques has become less effective. Then, using machine learning techniques on the physical layer will be more effective. In these two survey papers [50,51], the authors made a comprehensive survey and review of the latest studies related to security solutions based on machine learning in IoT environments. Table 3 presents the comparison between the papers related to ML-based security solutions in IoT.

Table 3. ML-based security solutions in IoT.

Ref.	Proposed Solutions	Techniques	Detection Approaches	Dataset	Complexity	Scalability	Accuracy	Result
[47]	A new framework depends on ML for different characterizations of network traffic. To determine and classify the baseline behavior of different devices in the IoT network.	- Joy tool Weka - Naive Bayes Multinomial classifier	Anomaly	Create their own dataset	-	-	99%	This paper explains that by depending on the network behavior, each IoT device connected to it can be accurately identified.
[48]	The authors proposed a new lightweight approach to detect DDoS malware in the environment of IoT.	- Convolutional neural network technique - Malware image classification	Anomaly	IoT malware dataset collected by IoTPOT	It is a complex system because it analyzes malware behavior.	It is a scalable system because it connects to a cloud server for deeper analysis.	94.0%	They proved the effectiveness of the proposed approach and that the approach could be modified to be more effective using different techniques to reduce the size of the network.

4.1.2. IDS-Based Security Solution in IoT

Many scientists have made efforts to develop IDS using regular methods on IoT networks. In this section, we studied works on IDS in IoT environments. U.D. Gandhi et al. proposed in [52] a new system called HIoTPOT, which refers to honeypot in the environment of IoT. They modified the architecture of IoT by adding honeypot and a fake system. Thus, when the new user wants to access the system if the entered user is an authenticated user the system will allow him to access a real system, but if the entered user is not authenticated, the system will send alerts to all IoT devices regarding the intruder, then it will allow him to access a fake system to monitor their behavior and understand the intruder's methodology. These collected records from unauthorized intruders are very useful to use when white hat hackers want to understand the behavior of real hackers to improve the weaknesses of the system and for research purposes. It is also useful for criminal evidence in any cybercrime. This is their proposed contributions to improve the IDS.

O.A. Okpe presented in [53] the common threads in IoT networks. Then, they discussed the vulnerabilities of IoT and attacks. Finally, they talked about the different proposed IDS in IoT networks. In [54], the authors made a survey of IDS for IoT-based smart environments, they presented the paradigm of IoT and its architectures, then they talked about IoT-based smart environments and smart cities. After that, they discussed the challenges of security in IoT. Then, they presented an overview of IDSs, the types of IDS, methods, and detection techniques. Finally, they discussed different IDS designed for the IoT environments.

In [55], the researchers proposed a new model to improve the home security system by using cameras to monitor any intruders. This camera automatically starts to record any movement of objects, then it analyzes the image to recognize the face of the intruder. If the intruder is one of the family members it ignores the alert, if he was an intruder and his face is not stored in its memory, it sends an alert via email to the house owner. In the email, it includes a recorded video of the intruders. This system is characterized by a lower cost compared to the traditional monitor systems. This system is effective in detecting intruders and alerting the house owners and guards. M.E. Pamukov and V.K. Poulkov [56] proposed a new model for IDS in IoT networks based on the Negative Selection Algorithm (NSA), and they called it Multiple Negative Selection Algorithm (MNSA). The main objective of this proposal is to reduce detection errors without the need for human interventions. Then, they compared the new proposed algorithm MNSA algorithm with the original NSA algorithm. They claimed that this algorithm gives a suitable solution for IDS in IoT.

In Cervantes et al. [57], a new IDS called INTI (IDS of Sinkhole attacks in 6LoWPAN for IoT) was suggested. It works to detect and identify the sinkhole attacks that prevent communication among network devices. It is one of the most destructive attacks on IoT networks. Midi et al. presented in [58] Kalis, a system for Knowledge-Driven Adaptable IDS in IoT. This system can detect different attacks widely through IoT systems in real-time. It can monitor many protocols at the same time; it is a spatial feature in the Kalis system. It could also be adapted in different network systems. After the evaluation of the Kalis system, authors approved that the latter is efficient in detecting different attacks to IoT systems. Thus, Kalis is considered an effective system.

In [59], the researchers proposed a distributed system to detect anomalies within the internal system for IoT networks where each node monitors the other nodes surrounding it. In addition to that, if it detects any abnormal behavior in one node, it will block the packet that comes from this node and send the report to its parent until they reach the root. This system works on the data link layer and network layer.

J.B. Karande and S.A. Joshi [60] conducted their study to evaluate the effectiveness of numbers of attacks detection algorithms used in the IoT and found that these algorithms were effective in the case of independent attacks. Yet, when many attacks occur and cooperate on IoT networks, these algorithms would be less effective in protecting the IoT networks. Finally, they recommended other researchers design a new algorithm that has a high ability to protect IoT networks from multi-pronged cooperated attacks.

The researchers in [53,54,61] defined the concept of IoT and its various detailed classifications and the number of attacks that can affect IoT networks. They also mentioned the advantages and disadvantages of some of the mechanisms used in the IoT, and the methods used in IDS mechanisms to detect and prevent attacks before they occur, preventing, thereby, the damage these attacks can cause. They also presented new vulnerabilities arising from IDS in IoT networks to help future researchers focus on important points and try to develop them.

L. Santos et al. analyzed and reviewed in [62] 20 research papers between 2009 and 2017 that propose IDS solutions of the IoT networks. From these reviewed studies, the authors concluded that the solutions offered are still in their infancy and cannot provide adequate protection against various attacks on IoT networks.

A. Sforzin et al. proposed in [63] a new scheme for IDS architecture on the IoT networks called RPiDS. Their proposal is based on Snort and Raspberry Pi. They discussed the effectiveness of used Snort and Raspberry Pi to build an IDS. Finally, the result of their experiment proved the effectiveness of using their proposal in different IoT environments from smart cities to smart homes.

In [64], the authors carried out a comprehensive study and review on the existing system for IDS and their rising systems, for example, the Internet of Vehicles (IoV). They reviewed and analyzed the existing IDS in the IoT environment based on:

i. Energy consumption.
ii. Performance and overhead computational.
iii. Privacy.

They determined the open challenges for newly made designs that might be collaborative and effective for the IDS and constrained the resource in the IoT system and its applications. The aim of this paper is to shed light on the open challenges and on the latest in the detection of intrusion in the IoT, to achieve efficient and effective IDS. In [65], the authors discussed Wormhole attacks which are mostly placed on the RBL network on the 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) adaptation layer. The Wormhole attack has four different operation models:

i. Encapsulation.
ii. Packet Relay.
iii. Out of Band Channel.
iv. High Power Transmission.

The authors proposed an IDS to improve security on IoT networks. They conducted their experiment using the Cooja simulator in Contiki open-source operating system. They used it to detect if there are any attacks on the value of Received Signal Strength Indicator (RSSI). Based on the results of their evaluation, they proposed that there is a great need to improve the positive detection rate. The rate of successful detection of attacks in their IDS was 90%. Table 4 presents the comparison between the papers related to IDS-based security solutions in IoT [52,55,56,62,63,66–69].

Table 4. IDS- based security solution in IoT.

Ref.	Proposed Solutions	Dataset	Threats	Detection Approaches	Techniques	Result
[52]	Proposed system called HIoTPOT refers to Honeypot in the environment of IoT.	They created two databases: authenticated users and the intruders' information behaviors.	Intruders.	Anomaly	- Raspberri Pi 3 as a server - MySQL database	HIoTPOT tracks authenticated and unauthenticated users to understand the behavior of the intruders, their methodology and purpose, in order to get a safe IoT environment in future.
[55]	Proposed a new model to improve the home security system by using cameras to monitor any intruders	-	Intruders.	-	- Raspberry Pi - Pi Camera Module - Passive Infrared (PIR) Motion Senor - Liquid Cristal Display (LCD) -Buzzer	Their proposal is beneficial for those who want to protect their properties. Moreover, tt is a very easy system that everyone can use.
[56]	Proposed new model for IDS in IoT network based on the NSA algorithm. They called the new algorithm MNSA.	-		Anomaly	- NSA - Artificial Immune System (AIS) - Negative Selection -Co-stimulation	They proposed MNSA which has satisfying results in simulation scenarios. However, this proposal needs more investigation before applying it in the real environment.
[62]	They proposed an IDS to improve security on IoT networks.	-	Wormhole attacks	-	- RSSI - Cooja simulator -Contiki OS	They got a success rate around 90% after applying their model to a small network.
[63]	New scheme for IDS architecture on the IoT networks called RPiDS.	Create their own dataset by simulating IoT networks traffic	Attacks	-	- Snort: network NIDS software. -Raspberry Pi	They proved the effectiveness of their proposed model in a distributed system as IoT, to serve the IDS.
[66]	They proposed ADS to monitor the null space and detected intrusions.	- In the learning phase, they used many attack-free datasets. - They created their dataset by Normal Operation Conditions (NOC).	- DoS attack - Integrity	Anomaly	- Hankel matrix - SSI - Tennessee–Eastman process	Their preliminary results proved the ability of their proposed model to the destination between DoS attacks and integrity attacks using the popular Tennessee–Eastman process.

Table 4. *Cont.*

Ref.	Proposed Solutions	Dataset	Threats	Detection Approaches	Techniques	Result
[67]	They improved the detection system for (DDoS).	They created their own dataset for DDoS attacks.	DDoS attacks	Anomaly	- Raspberri Pi 3 as a server - CEP technique	- CEP improves the performance of detection of DDoS attacks in real-time on IoT. - It reduced the computational power when they executed it on devices.
[68]	Proposed a new framework which collaborate between signature-based IDS and blockchain techniques in the IoT.	-	- Worm attack - Flooding attack	Signature-based IDSs (Misuse)	- Blockchain - Collaborative IDS (CIDSs)	The results of the evaluation for CBSigIDS proved the effectiveness and robustness of the signature-based detection.
[69]	Combined the encryption by CP-ABE, IDS, and IRS.	-	Malicious packets	Signature-based IDS and anomaly-based IDS	- Used GMP from Python library to perform the cryptographic. - CP-ABE	They proved the effectiveness of their proposed model CP-ABE which ensures the correct encryption of communication between devices which are connected to the network. Moreover, security increased by using this model.

4.2. Security Solutions in Other Environments

This section presents studies related to the security solutions in other environments.

ML-Based IDS

The different networks in the world may get exposed to different kinds of attacks, so these networks need smart IDS to protect them. In this section, we present studies that use ML to improve IDS in different environments. The authors mention in [70] that the increasing use of high-speed Internet made the detection of attacks a major challenge to traditional IDS. Therefore, it became necessary to use AI techniques to develop IDS and make it fit to the high speed networks. AI techniques train IDS to detect intrusions and give it the ability to adapt and learn, which contributes to raise their efficiency and make them discover new types of intrusions.

The authors in [71] applied different ML techniques on the computer network to detect the attacks. They studied different kinds of attacks: SSH brute force, MITM, and DDoS attacks. What they derived from this study was the effectiveness of applied and used ML techniques in protecting networks. In [72], the authors proposed a new model of IDS called Spark-Chi-SVM. They used it for feature extraction the ChiSqSelector tool. They built their model on Apache Spark using a Support Vector Machine (SVM) classification ML algorithm on the Big Data platform. To evaluate the model, they used the KDD99 dataset in testing and training the model. After that, they compared their proposed model Chi-SVM and Chi-Logistic Regression ML algorithm. The results of their model evaluation were as the follows:

i. High performance.
ii. Effectiveness on a big data platform.
iii. Reduction the time needed for training.

5. IDS for IoT Security

This section presents the studies related to the IDS for IoT security based on ML and DL.

5.1. ML-Based IDS for IoT Security

After the debut and wide spread of IoT, the traditional IDS did not provide the necessary protection. Therefore, it became necessary to apply AI techniques to develop an IDS that is compatible with IoT networks, to protect them from intrusion. In this section, we present studies that applied techniques of ML on IDS to improve the security in IoT environments.

P. Li and Y. Zhang in [73] proposed a new model to improve the security in IoT environments. They improved the DBN algorithm and used it in order to get the optimal structure of the network by multiplying iterations with the applied Genetic Algorithm (GA). Then, they chose the optimal structure of the network with DBN for IDS. They got a high level of accuracy and they effectively improved the rate of intrusion detection.

In [74], the authors mentioned the concerns about the consumption of energy and security in IoT. Therefore, they proposed three algorithms. The first one is named ULEACH clustering algorithm; it combines the IDS and clustering algorithm to put IDS on the head of cluster nodes to improve IDS, and this improved the LEACH protocol. The second algorithm was used to improve energy consumption depending on game theory. The third algorithm was intended to achieve a balance between effective IDS and energy consumption. It is a modified version of the particle swarm optimization (PSO). Their experiment resulted in the improvement of energy consumption and more effectiveness of the IDS performance.

V. Kumar et al. proposed in [75] a new model that unified IDS to improve security in the IoT environment. They used the UNSW-NB15 dataset to train their model. Then, they compared their model and other existing models, which were trained on the same dataset; these models were ENADS and DENDRON. In addition, they compared their model with other ML techniques. The accuracy of the new model was higher than the two existing

models, ENADS and DENDRON, and it has an effective role in improving IDS and security if IoT environment.

In [76], the authors discussed the main challenges in IDS for wireless in IoT network. Then, they reviewed the concepts of active learning and its applications. Finally, they proposed a new model to adapt active learning techniques on the IDS for wireless in the IoT network. After they evaluated their model, they noted significant improvements for IDS based on active learning techniques compared with the traditional techniques of supervised learning for IDS. In [77], the authors compared different algorithms of ML to get better accuracy on the IDS. These algorithms were SVM, Artificial Neural Network, Decision Tree, Logistic Regression, and Random Forest. The best accuracy was 99.4% for the Decision Tree algorithm.

N. Chaabouni et al. carried out a deep survey [78] of different IoT network studies and security issues. They discussed IoT network challenges and threats. Their survey focused on IDS in IoT network. They reviewed different techniques that were applied to IDS in the IoT network; the ML techniques and the traditional techniques. Furthermore, they discussed the different proposed architectures for IDS in the IoT network, their detection approaches, algorithms, and strategies. Finally, they stated that their paper will help future researchers in IDS in the IoT network area. L. Deng et al. analyzed in [79] the issues and characterizations of security in IoT networks. They talked about the importance of IDS in IoT. They discussed different types of IDS and their applications. Then, they compared the different applications of IDS. They also considered that improving the IDS using ML techniques and data mining techniques is an exciting domain for future research. Finally, they proposed a new scheme for IDS in IoT environment, which combines two algorithms: Principal Component Analysis (PCA) and Fuzzy C-means clustering algorithm (FCM). The results of their proposed scheme simulation improved the effectiveness of the detection process and reduced the False Positive Rate (FPR).

In [80], the authors analyzed different types of attacks on an Ad Hoc On-Demand Distance Vector (AODV) network. They generated datasets with the NS2 simulator on three different AODV networks. Their experimentations were based on three datasets: worm hole dataset, black hole dataset, and flooding attack dataset. After that, they used the data mining techniques to classify the data obtained from the trace files after simulating the network using WEKA software. They used different algorithms for the analysis. The used algorithms were Decision Table, Naïve Bayes, BayesNet, and Random Tree. They analyzed the AODV network under different attacks and presented the result of each of them. In [81], the authors suggested a new and intelligent architecture to improve smart home security in IoT environment. The IDS architecture contains three main layers; each layer has a specific function.

i. The first layer assorts the type of each IoT device and defines its normal behavior using MAC address.
ii. The second layer monitors and detects widespread wireless attacks against IoT devices that are connected to the network.
iii. The third layer categorizes the attack that was deployed depending on their types.

They used a supervised technique to detect different popular types of cyber-attacks on IoT networks. Their proposal composed of three key functions:

i. Recognizing and classifying the normal behavior of each device connected to the IoT network.
ii. When the attack occurs, it identifies malicious packets on the network.
iii. It can classify any attack when it appears. They use it to evaluate their smart home system framework which contains eight commercial smart devices.

Finally, they conducted an experiment to evaluate the performance of this architecture. Their results were satisfying and indicated the effectiveness and efficiency of the proposed architecture. They evaluated the IDS architecture by distributing twelve attacks from four main different categories of network attacks such as Spoofing, DoS, Reconnaissance, MITM,

and Replay. They evaluated their IDS architecture based on four scenarios of multi-layer attacks. Their proposed architecture can identify each IoT device and the network activities to determine whether the behavior is normal or malicious. Furthermore, it detects any attacks on the IoT networks. In [82], the authors created their dataset depending on the WSN by capturing the information from sent and received packets on the network. They used the Wireshark tool for captured data. Then, they proposed a new model for the IDS by combining two ML algorithms, an SVM algorithm for classification, and a K-means clustering algorithm. The new proposal improved the rate of detection and reduced the FPR. P. Shukla proposed in [83] three models for IDS based on ML techniques. The first model is called KM-IDS; it uses an unsupervised ML technique. It is a K-means clustering algorithm for the IDS. The second model was the IDS based on a supervised ML technique; it is a decision tree algorithm called DT-IDS. The third model was an IDS based on a hybrid system between a supervised ML technique and an unsupervised ML technique. He combined K-means clustering algorithm and decision tree algorithm called the model ML-IDS. The detection rate for each model was:

i. KM-IDS = 70–93%
ii. DT-IDS = 71–80%
iii. ML-IDS = 71–75%

The third model, ML-IDS, had the best accuracy and FPR. In [84], the authors proposed a new model for IDS based on supervised ML. They came up with an enhanced version of SVM technique called c-SVM. The result of their model accuracy was 100% when it was evaluated on the same network topology with unknown data accuracy, and 81% when their model was evaluated on the different network topology with unknown data. In [85], the authors suggested a new model to improve the security of IoT middleware. Their model was an IDS based on the J48 ML algorithm to protect IoT middleware from DoS threats. The results of their evaluation were:

i. Average accuracy = 73.52%
ii. Capture rate for packet = 73.52%
iii. Network packets capture by IDS = 75%
iv. Alerts = 18.05%
v. Packet categorized average time = 0.0351 s
vi. The average usage of CPU = 16%.

S. Zhao et al. proposed in [86] a new model for IDS depending on classifier and dimension reduction algorithm. To reduce the dimension of the dataset by reducing its features, they used PCA. For the classifier, they combined K-nearest neighbor algorithms and Soft-Max regression to build the classifier. The evaluation result approved the effectiveness of their proposed model. In addition, the time of performance and complexity of computing approved the affectedness of a new model in detected intrusions. Table 5 presents the comparison between papers related to ML-based IDS for IoT security [27,73–75,77,79–90].

Table 5. ML-based IDS for IoT security.

Ref.	Dataset or Environment	Threats	Detection Approaches	Techniques	Accuracy
[27]	-	Attacks Intruders	Anomaly	-Protocol used Zero-Knowledge Proofs (ZKP) -Elliptic Curve Discrete Logarithm Problem (ECDLP) -Cloud Analyst tool	-
[73]	KDDCUP	- DoS - Remote to local attack (R2L) - Probing (Probe) - User-to-Root (U2R)	Hybrid	- Their evaluation is based on simulation. - Improved DBN - GA	99%
[74]	They used Deter Lab platform to evaluate their experiment.	- Attacks - Attackers - Intruders	Hybrid	- Deter Lab platform - LEACH protocol - Clustering algorithm - PSO - Mixed strategy Nash equilibrium solution	-
[75]	UNSW-NB15	- Exploit - Dos - Probe - Generic	Signature-based IDSs (Misuse)	- Decision tree - C5 - CHAID - CART - QUEST - Neural network - SVM	88.92%
[77]	DS2OS from Kaggle	- DoS - Data Type Probing (DP) - Malicious Control (MC) - Malicious Operation (MO) - Scan (SC) - Spying (SP) - Wrong Setup (WS) - Normal (NL)	Anomaly	- SVM - Artificial Neural Network - Decision Tree - Logistic Regression - Random Forest	99.4%
[79]	KDDCUP99 data set	- Normal - DoS - Probing - R2L - U2R5	Anomaly	- K-means clustering algorithm - PCA algorithm - FCM algorithm	-

Table 5. *Cont.*

Ref.	Dataset or Environment	Threats	Detection Approaches	Techniques	Accuracy
[80]	Three datasets generated by NS2 simulator. -Worm hole dataset -Black hole dataset -Flooding attack dataset	- Worm hole, black hole, and flooding attacks.	-	- Decision Table algorithm - Naïve Bayes algorithm - Bayes Net algorithm - Random Tree algorithm	-
[81]	They collected their data using tcpdump tool.	- DoS - DDoS/Botn - MITM. - Spoofing - Insecure Firmware - Data Leakage	Anomaly	- Supervised ML - tcpdump tool - secure shell (SSH) - Syslog Server	-
[82]	They collected their data set from WSN using Wireshark tool.	Attacks Intruders	-	-SVM -K-mean	-K-mean = 71.45% -SVM = 74.45 % -(SVM + K-mean) = 98.34%
[83]	Simulated on RPL based 6LoWPAN networks	Wormhole attacks	Anomaly	- K-means clustering algorithm - Decision tree algorithm	The third model ML-IDS gets the best accuracy and FPR.
[84]	-	-	Anomaly	SVM.	81% accuracy on the different network topology with unknown data.
[85]	Create their own dataset	DoS.	Anomaly	J48 Algorithm	Average accuracy = 73.52%
[86]	KDD Cup 99 dataset	- Probing Attack - DoS Attack - U2R Attack - R2L Attack	Anomaly	-Softmax regression -K-nearest neighbor algorithms -Dimension reduction algorithm - PCA	3 features = 84.999% 6 features = 84.436% 10 features = 84.406%
[87]	Create their own dataset	Distributed denial of service (DDoS) attacks	Anomaly	Logistic Model Trees (LMT)	Between 99.92%–99.99%
[88]	Create their own dataset	IoT attacks	Hybrid	Improved the MUD framework by developed an SDN-based system empowered by machine learning.	The higher accuracy was 97.5.

Table 5. *Cont.*

Ref.	Dataset or Environment	Threats	Detection Approaches	Techniques	Accuracy
[89]	Create their own dataset	Iot attacks	Anomaly	Developed a classification scheme using a set of device-specific clustering models.	More than 94%
[90]	Create their own dataset	DDoS attacks	Anomaly	Detecting anomalies based on boosting machine learning method.	It has the ability to distinguish between the legitimate traffic profile and DDoS traffic by observed the traffic deviations, as well as having high accuracy.

5.2. DL-Based IDS for IoT Security

This section presents studies that applied techniques of DL to IDS to improve the security in IoT environments. In paper [91], the authors applied DL techniques for the IDS. Their main objective is to reduce the anomaly attacks on IoT network traffic. Y. Zhang et al. suggested in [92] a new model for IDS by developing DBN and GA. Their model improved IDS effects on the network every time it faced more than one kind of attack. In [93], the researchers proposed a new model based on DL to detect attacks in IoT networks. They noted that the distributed attack detection system gives better results than using a centralized attack detection system. They used DL mechanisms because they found out that they are better and give more accurate results in cyber security areas. In addition to that, DL techniques have a high ability to extract features. The authors applied in [94] an artificial neural network technique on their dataset to test its abilities to detect intrusion on IoT networks. Their experience obtained good results, which proves the effectiveness of using DL technique in the development of IDSs.

DL-Based MDS for IoT Security

Researchers and developers are very interested in developing MDS in IoT environments. They made great efforts to develop these systems and obtain a high accuracy and efficiency for MDS. This contributes to the improvement of the security and privacy of the IoT systems. In this section, we review the latest studies in this field.

In [95], the authors carried out a comprehensive review of different approaches for MDS. Then, they mentioned the advantages and disadvantages of each approach. After they carried out the review, they stated that, up to now, there are huge gaps in this area. Finally, they suggested combining more than one approach together to get a more effective model. F. Xiao et al. proposed in [96] a model for a MDS based on DL called BDLF which combines behavior graphs of API calls with the SAEs model. In their proposed model, they used the Stacked Autoencoders (SAEs)—DL techniques—for high-level features extraction from behavior graphs and traditional ML algorithms Decision Tree (DT), KNN, Naïve Bayes (NB), and SVM which called SAE-DT, SAE-KNN, SAE-NB, and SAE-SVM for the classification. The results of the experiment showed an improvement in the detection precision of the model. The result of their experiment improved the average of accuracy by 1.5%.

In [97], the authors created the IoT malware dataset then used operation codes (OpCodes) for extraction the features. After that, they applied a RNN DL algorithm to train and test their model. They compared the result of applying DL algorithms with the traditional ML algorithms. The result of their experiment gave a high accuracy of 98.18%, and the result of their comparison revealed that DL gives better results.

The authors proposed in [98] a new model based on DBN DL techniques. After that, they compared these techniques, traditional shallow neural networks, and the traditional ML techniques, decision trees, SVM, and the KNN algorithm. They got the best accuracy after applying DBS; it was 96%. In paper [99], an MDS based on DL was proposed. In order to improve the performance, they used image recognition techniques to concert the malicious code to grayscale images. This new model of malware detection is based on a CNN. This model improved the accuracy and speed.

Table 6 presents a comparison between studies related to IoT MDS based on DL [48,96–100]. This comparison is of proposed solutions, techniques, ML/DL, detection approaches, dataset, scalability, and results.

Table 6. Comparison between studies related to IoT MDS based on DL techniques.

Ref.	Proposed Model	Algorithms	Feature Extraction Techniques	Accuracy	FAR	Dataset	Open Challenges
[48]	Novel light-weight approach for detecting DDos malware in IoT environments.	CNN for classification	Malware image to convert from malware binary to image to use in future for feed the classification algorithm	94.0% (goodware and one family of DDoS malware) 81.8% (goodware and two main malware families)	-	IoT malware dataset collected by IoTPOT	- Proposed system that has less computation resources to implement on IoT devices. - Proposed a new malware image extraction method to get more representative features of malware for classification.
[96]	Proposed four models SAE-SVM, SAE-DT, SAE-NB, and SAE-KNN.	- SVM - DT - NB - KNN	SAEs	Improved the average of precision by 1.5%.	-	Collecting malware samples by vx_heaven	Improved the SAEs model to apply in MDS and classification.
[97]	Used DL algorithms on MDS then compared their result with traditional ML algorithms.	- RNN	- OpCodes	High accuracy 98.18%		Creating the IoT malware dataset	Improved the accuracy, speed, and scalability of IoT MDS.
[98]	Proposed a new MDS model based on DBN.	- DBN	- DBN	96%	-	Building unlabeled malware dataset	Investigated how the huge data affects DBN performance.
[99]	Proposed a new MDS model based on CNN.	Image recognition Bat Algorithm	- CNN	94.5%	-	Malware image data from Vision Research Lab	Merged their model with the SPP-net model. - Conversion of malicious code into color images
[100]	Novel detection method to detect previously unseen malware based on OpCode graph.	KNN and SVM.	- Graph extraction - Graph embedding	KNN (K = 10) = 95.09 SVM = 95.62 Adaboost = 96.09 Decision Tree = 92.90	For (10%) KNN (K = 10) = 3.06 SVM = 2.25 Adaboost = 2.65	Collecting malware samples by vx_heaven	Malware detection in computer security.

Table 7 presents a comparison and a summary of studies on ML and DL for IoT malware detection. Table 8 presents the comparison between studies related to DL for MDS in IoT based on numbers of parameters.

Table 7. Comparison of related work on DL for malware detection in IoT.

Ref.	Accuracy (%)	Detection Rate	DL									Attack Surfaces Secured			Attacked Detected
			SAEs	ANNs	CNNs	RNNs	AEs	RBMs	DBNs	GANs	EDLNs	PerceptionLayer	Networklayer	ApplicationLayer	
[48]	√	-	-	-	√	-	-	-	-	-	-	√	-	-	DDoS Malware
[77]	√	√	-	√	-	-	-	-	-	-	-	-	-	-	Malware Families
[96]	-	√	√	-	-	-	-	-	-	-	-	-	√	-	Malware Families
[97]	√	-	-	-	-	√	-	-	-	-	-	-	-	√	Malware Families
[98]	√	-	-	-	-	-	-	-	√	-	-	-	√	-	Malware Families
[99]	√	√	-	-	√	-	-	-	-	-	-	-	√	-	Malware Families
[101]	√	√	-	√	-	-	-	-	-	-	-	-	√	-	Malware Families
[102]	√	-	-	-	-	-	-	-	-	√	-	-	-	√	Zero-day malware
[103]	√	√	-	√	√	√	-	-	-	-	-	-	√	-	Ransomware Malware
[104]	√	√	-	√	-	-	-	-	-	-	-	-	√	-	DDoS Malware
[105]	√	√	-	-	-	√	-	-	-	-	-	√	-	-	Ransomware Malware
[106]	√	√	-	-	-	-	-	-	√	-	-	-	-	√	Malware Families
[107]	√	√	-	-	√	-	-	-	-	-	-	-	√	-	Intelligent Malware

Table 8. Comparison of related works on DL for malware detection in IoT based on number of parameters.

Ref.	Classifier	Accuracy (%)	Recall & Detection Rate (%)	F1-Score (%)	Precision (%)	Error Value		
						MAE	MSE	RMSE
[48]	CNN	94.0	94.67	-	-	-		
[96]	SAE-DT	-	99.2	98.9	98.6	-	-	-
[97]	RNN (LSTM)	94.0	-	-	-	-	-	-
[98]	DBN-decision tree	96.0	-	96.0	-	-	-	-
[99]	CNN	94.5	94.5	-	94.6	-	-	-
[102]	Deep autoencoder (DAE +GAN)	95.74	-	-	-	-	-	-
[103]	Neural Networks	75.93	73.33	67.01	61.68	-	-	-
[105]	ARI-LSTM	93.0	-	-	-	-	-	-
[106]	DBN	96.76	97.84	-	95.77	-	-	-
[107]	CNN	96.6	98.4	96.2	94.0	-	-	-
[107]	DNN	91.0	91.1	90.9	90.6	-	-	-
[108]	ANN	86.0	-	-	-	-	0.041	0.202
[109]	Neural Network	91.14	95.01	93.32	-	-	-	0.3983
[109]	Multiple Association Rule	66.70	78.84	79.74	-	-	-	0.5747
[109]	Bayesian	84.11	94.89	85.98		0.1695		0.3668
[110]	RNN	96.01	-	-	-	-	-	-
[111]	Random forest	89.03	98.0	94.2	98.0	0.1097	-	-
[111]	SVM	85.43	85.5	85.4	85.3	0.1532	-	-

In fact, the field of research in the MDS based on DL in IoT environments is still a new field that needs more research and studies. Moreover, it needs development and improvement in several aspects such as detection rate and accuracy to obtain high security IoT environments and to maintain the privacy of users to gain their confidence and increase their reliance on IoT environments. This will contribute to achieving the main goal of IoT which is to obtain comfort and security for users. Therefore, it is necessary to propose a robust MDS based on DL that has a high ability to detect renewable malware by getting MDS work as a human mind to solve the problem of security in IoT environments.

6. Analysis and Discussion

Many scientists, developers, and researchers were interested in securing the IoT environment and made great efforts in this field. One of the methods that they used to improve the security in IoT environments and protect them from any malware or prevent the latter from harming IoT environments is MDS. The use of this type of system can significantly reduce the spread of malware that may cause malfunctions of IoT systems and violate the privacy of users. The researchers were interested in developing MDS because if we get more accurate and efficient MDS, we will obtain high-security IoT environments.

In IoT environments, hackers may use intelligent malware to damage the IoT environments. Therefore, using AI to build MDS had a major role in developing the efficiency and effectiveness of MDSs and providing them with the ability to predict and distinguish. Scientists and researchers have conducted much research and many studies in the field of using ML techniques to develop MDS, and they have obtained good results. With the advent of DL, scientists and researchers have paid attention to use the DL techniques in developing MDSs to obtain highly accurate and efficient systems. Table 7 presents the summary of the studies that focus on the use of DL techniques in developing MDS.

We also note the interest of many scientists in improving MDS accuracy. Some of them were interested in improving the detection rate and reducing the error rate.

Table 8 presents the comparison of many scientists' studies and research based on a number of parameters: accuracy, recall and detection rate, f1-score, precision, MAE, MSE, and RMSE. Some researchers obtained a high accuracy, but they did not improve the other parameters as in [110] while others, such as [96], got a high detection rate, recall, f1-score, and precision but they did not improve the accuracy. Therefore, to get a robust model for MDS, we recommend improving all these parameters all together at the same time.

7. Findings

In this paper, more than 100 research papers were summarized and the various efforts of scientists and researchers in this field were reviewed and compared. Based on the previous studies, it appears to us that there is a need to propose a new framework that has a high ability to:

a. Predict and distinguish malicious software from ordinary data automatically,
b. Deal with the nature of the various IoT data,
c. Improve energy savings and time consumed. To be appropriate and work efficiently with IoT devices, it should be that most of them are characterized by their simplicity and lightness,
d. Find a solution for IoT devices that are in the current market and lack the security aspect, and
e. Propose new IoT architecture which is more efficient and effective.

Many gaps are noticed in MDSs that are based on DL in IoT environments.

Some scientists and researchers recommended to continue the research in this field and apply different techniques and proposed new MDS with high accuracy to improve the malware detection rate, in contemplation of obtaining a safe IoT environments with high security and privacy that can be trusted by humans, and to achieve the objective of IoT and smart cities making human life more comfortable and intelligent. A. Khraisat et al. [112] disclosed that many researchers and scientists did a lot of research in the field of

IDS, but we still need more research in MDS to improve accuracy, detection rate, and other parameters.

8. Conclusions

The IoT is a very interesting area and it is the future of humanity. On the other hand, malware is evolving day-by-day with AI, which raises concerns about security in IoT environments and maintaining users' privacy. Therefore, both scientists and researchers have made great efforts to raise the level of security in IoT environments. This paper presents a number of comparisons between previous studies. Still, there is a need for more research and more studies to be conducted in this field to overcome malware and prevent it from causing any harm to the IoT environment. This paper serves as a link between the researchers and the latest existing studies, making it easier for researchers to know the latest developments in this field and thus helping them develop more effective contributions.

In future work, we will suggest a robust framework for a MDS based on DL techniques to improve security in IoT environments. Moreover, we will work to improve all the mentioned parameters, accuracy, recall and detection rate, f1-score, precision, MAE, MSE, and RMSE, to get a strong model.

Author Contributions: Conceptualization, H.T.; Data curation, H.T.; Formal analysis, H.T.; Funding acquisition, H.T.; Investigation, H.T.; Methodology, H.T.; Project administration, H.T.; Resources, H.T.; Software, H.T.; Supervision, H.T. and R.Z.; Validation, H.T.; Visualization, H.T.; Writing —original draft, H.T.; Writing—review & editing, H.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received funding from SAUDI ARAMCO Cybersecurity chair.

Acknowledgments: We would like to thank SAUDI ARAMCO Cybersecurity Chair for funding this project.

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

Abbreviations

The following abbreviations are used in this manuscript:

IoT	Internet of Things
Ref.	References
MDS	Malware Detection System
IDS	Intrusion Detection System
ADS	Anomaly Detection System
DNN	Deep Neural Network
DT	Decision Tree
EL	Ensemble Learning
RBMs:	Restricted Boltzmann Machines
MUD	Manufacturer Usage Description
AI	Artificial Intelligence
ML	Machine Learning
DoS	Denial of Service
DDoS	Distributed Denial of Service
AEs	Auto-encoders
EDLNs	Ensemble Deep Learning Networks
GAN	Generative Adversarial Network
KNN	K-Nearest Neighbor
RF	Random-Forest
SDN	Software Defined Networking
CNN	Convolutional Neural Network
Ars	Association Rules
DL	Deep Learning

NB	Naive Bayes
PCA	Principal Component Analysis
SAEs	Neural Network-Stacked AutoEncoders
DBN	Deep Belief Network
ANN	Artificial Neural Network
SVMs	Support Vector Machines

References

1. Statista Research Department. "Number of IoT Devices 2015–2025," Statista. 2016. Available online: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (accessed on 5 June 2021).
2. Lewis, T. *IDS vs. IPS: How Each System Works and Why You Need Them*; LBMC: Chattanooga, TN, USA, 2019; Available online: https://www.lbmc.com/blog/ids-vs-ips/ (accessed on 15 June 2021).
3. Kaspersky. *IoT under Fire: Kaspersky Detects more than 100 Million Attacks on Smart Devices in H1 2019*; Kaspersky: Moscow, Russia, 2019; Available online: https://www.kaspersky.com/about/press-releases/2019_iot-under-fire-kaspersky-detects-more-than-100-million-attacks-on-smart-devices-in-h1-2019 (accessed on 8 June 2021).
4. Clark, J. *What Is the Internet of Things?* IBM: Armonk, NY, USA, 2016; Available online: https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/ (accessed on 17 June 2021).
5. Oracle. *What Is IoT?* Oracle: Austin, TX, USA, 2020; Available online: https://www.oracle.com/internet-of-things/what-is-iot.html (accessed on 5 June 2021).
6. Burhan, M.; Rehman, R.A.; Khan, B.; Kim, B.S. IoT elements, layered architectures and security issues: A comprehensive survey. *Sensors* **2018**, *18*, 2796. [CrossRef]
7. Sethi, S.R.; Pallavi, S. Internet of Things: Architectures, Protocols, and Applications. *J. Electr. Comput. Eng.* **2017**, *25*. [CrossRef]
8. Sethi, S.R.; Sarangi, P. Internet of Things: Architectures, Protocols, and Applications. Available online: https://www.hindawi.com/journals/jece/2017/9324035/ (accessed on 7 June 2021).
9. Atzori, L.; Iera, A.; Morabito, G.; Nitti, M. The social internet of things (SIoT)—When social networks meet the internet of things: Concept, architecture and network characterization. *Comput. Netw.* **2012**, *56*, 3594–3608. [CrossRef]
10. Calihman, A. Architectures in the IoT Civilization, Netburner. 2019. Available online: https://www.netburner.com/learn/architectural-frameworks-in-the-iot-civilization/ (accessed on 1 July 2021).
11. Smith, A. The Five Biggest Security Threats and Challenges for IoT, DZone. 2020. Available online: https://dzone.com/articles/the-biggest-security-threats-and-challenges-for-io. (accessed on 15 July 2021).
12. Perry, J.S. Anatomy of an IoT Malware Attack. 2019. Available online: https://www.ibm.com/developerworks/library/iot-anatomy-iot-malware-attack (accessed on 17 July 2021).
13. Grimes, M.A. 9 Types of Malware and How to Recognize Them, Cso. 2019. Available online: https://www.csoonline.com/article/2615925/security-your-quick-guide-to-malware-types.html (accessed on 9 July 2021).
14. JOHN. Malware Types and Classifications, Lastline. 2018. Available online: https://www.lastline.com/blog/malware-types-and-classifications/ (accessed on 22 June 2021).
15. Idika, N.; Mathur, A.P. A Survey of Malware Detection Techniques. Available online: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.75.4594&rep=rep1&type=pdf (accessed on 15 July 2021).
16. Whitman, M.E. Principles of Information Security. In *Security Technology: Intrusion Detection and Prevention Systems, and Other Security Tools*, 5th ed.; Cengage Learning: Boston, MA, USA, 2014; p. 677. ISBN 978-1-2854-4836-7.
17. Petters, J. IDS vs. IPS: What Is the Difference? Varonis, Security Blog. 2018. Available online: https://www.varonis.com/blog/ids-vs-ips/ (accessed on 22 June 2021).
18. Kumar, B.S.; Raju, T.C.S.P.; Ratnakar, M.; Baba, S.D.N. Sudhakar Intrusion Detection System-Types and Prevention. *Int. J. Comput. Sci. Inf. Technol.* **2013**, *4*, 77–82.
19. Aljawarneh, S.; Aldwairi, M.; Yassein, M.B. Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. *J. Comput. Sci.* **2018**, *25*, 152–160. [CrossRef]
20. West, M. Preventing System Intrusion. In *Network and System Security*, 2nd ed.; Vacca, J.R., Ed.; Syngress: Boston, MA, USA, 2014; pp. 29–56.
21. Point, C. Smart Cities Need Smart Security. Itone. 2017. Available online: https://www.itone.lu/actualites/smart-cities-need-smart-security. (accessed on 8 November 2019).
22. Din, I.U.; Guizani, M.; Rodrigues, J.J.P.C.; Hassan, S.; Korotaev, V.V. Machine learning in the Internet of Things: Designed techniques for smart cities. *Futur. Gener. Comput. Syst.* **2019**, *100*, 826–843. [CrossRef]
23. Popescul, D.; Radu, L.D. Data Security in Smart Cities: Challenges and Solutions. *Informt. Econ.* **2016**, *20*, 29–38. [CrossRef]
24. Baig, Z.A.; Szewczyk, P.; Valli, C.; Rabadia, P.; Hannay, P.; Chernyshev, M.; Johnstone, M.; Kerai, P.; Ibrahim, A.; Sansurooah, K.; et al. Future challenges for smart cities: Cyber-security and digital forensics. *Digit. Investig.* **2017**, *22*, 3–13. [CrossRef]
25. Mehta, V.; Bansal, P.; Mohit, K.; Banerjee, P. Empowering the Security for Iot-Based Communications in Smart City. *Int. Conf. Autom. Comput. Eng. ICACE* **2019**, 57–60. [CrossRef]
26. Bohli, J.M.; Skarmeta, A.; Victoria Moreno, M.; Garcia, D.; Langendorfer, P. SMARTIE project: Secure IoT data management for smart cities. *Int. Conf. Recent Adv. Internet Things RIoT* **2015**, *13*, 7–9. [CrossRef]

27. Djigal, H.; Jun, F.; Lu, J. Secure Framework for Future Smart City. In Proceedings of the 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), New York, NY, USA, 26–28 June 2017; pp. 76–83. [CrossRef]
28. Pacheco, J.; Hariri, S. IoT security framework for smart cyber infrastructures. In Proceedings of the 2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W), Augsburg, Germany, 12–16 September 2016; pp. 242–247. [CrossRef]
29. Khatoun, R.; Zeadally, S. Cybersecurity and privacy solutions in smart cities. *IEEE Commun. Mag.* **2017**, *55*, 51–59. [CrossRef]
30. Cui, L.; Xie, G.; Qu, Y.; Gao, L.; Yang, Y. Security and Privacy in Smart Cities: Challenges and Opportunities. *IEEE Access* **2018**, *6*, 46134–46145. [CrossRef]
31. Alrashdi, I.; Alqazzaz, A.; Aloufi, E.; Alharthi, R.; Zohdy, M.; Ming, H. AD-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning. In Proceedings of the 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 7–9 January 2019; pp. 305–310. [CrossRef]
32. Balla, P.B.; Jadhao, K.T. IoT Based Facial Recognition Security System. *Int. Conf. Smart City Emerg. Technol. ICSCET* **2018**, *7*, 1–4. [CrossRef]
33. Garcia-Font, V.; Garrigues, C.; Rifà-Pous, H. Attack classification schema for smart city WSNs. *Sensors* **2017**, *17*, 771. [CrossRef] [PubMed]
34. Aloqaily, M.; Otoum, S.; AI Ridhawi, I.; Jararweh, Y. An intrusion detection system for connected vehicles in smart cities. *Ad Hoc Netw.* **2019**, *90*. [CrossRef]
35. Elsaeidy, A.; Munasinghe, K.S.; Sharma, D. A Machine Learning Approach for Intrusion Detection in Smart Cities. In Proceedings of the 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), Honolulu, HI, USA, 22–25 September 2019; pp. 1–5.
36. Vaidya, V.D.; Vishwakarma, P. A Comparative Analysis on Smart Home System to Control, Monitor and Secure Home, based on technologies like GSM, IOT, Bluetooth and PIC Microcontroller with ZigBee Modulation. *Int. Conf. Smart City Emerg. Technol. ICSCET* **2018**, *11*, 1–4. [CrossRef]
37. Cvitić, I.; Peraković, D.; Periša, M.; Gupta, B. Ensemble machine learning approach for classification of IoT devices in smart home. *Int. J. Mach. Learn. Cybern.* **2021**. [CrossRef]
38. Aalsalem, M.Y.; Khan, W.Z.; Gharibi, W.; Armi, N. An intelligent oil and gas well monitoring system based on Internet of Things. In Proceedings of the 2017 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET), Jakarta, Indonesia, 23–24 October 2017; pp. 124–127. [CrossRef]
39. Valencia, C.M.P.; Alzate, R.E.; Castro, D.M.; Bayona, A.F.; Garcia, D.R. Detection and isolation of DoS and integrity attacks in Cyber-Physical Microgrid System. In Proceedings of the 4th IEEE Colombian Conference on Automatic Control, Medellin, Colombia, 15–18 October 2019. [CrossRef]
40. Qin, H.; Han, Z. Crude-Oil Scheduling Network in Smart Field Under Cyber-Physical System. *IEEE Access* **2019**, *7*, 91703–91719. [CrossRef]
41. Mualla, Y.; Najjar, A.; Boissier, O.; Galland, S.; Tchappi Haman, I.; Vanet, R. A Cyber-Physical System for Semi-Autonomous Oil&Gas Drilling Operations. In Proceedings of the 4th IEEE Colombian Conference on Automatic Control, Medellin, Colombia, 15–18 October 2019; pp. 514–519. [CrossRef]
42. Khan, W.Z.; Aalsalem, M.Y.; Gharibi, W.; Arshad, Q. Oil and Gas monitoring using Wireless Sensor Networks: Requirements, issues and challenges. In Proceedings of the International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications, Jakarta, Indonesia, 23–24 October 2017; pp. 31–35.
43. Chen, X.; Fan, J.; He, Q.; Wang, Y.; Liu, D.; Hu, S. Economical and balanced production in smart Petroleum Cyber–Physical System. *Futur. Gener. Comput. Syst.* **2019**, *95*, 364–371. [CrossRef]
44. Wadhawan, Y.; Neuman, C. Defending cyber-physical attacks on oil pipeline systems: A game-theoretic approach. In Proceedings of the 1st International Workshop on AI for Privacy and Security, New York, NY, USA, 29–30 August 2016. [CrossRef]
45. Lakhanpal, V.; Samuel, R. Implementing blockchain technology in oil and gas industry: A review. In Proceedings of the SPE Annual Technical Conference and Exhibition, Dallas, TX, USA, 24–26 September 2018. [CrossRef]
46. Sethii, P.; Chawla, M.; Dutta, K.; Sharma, M.; Gupta, S. Security framework for data aggregation in sensor cloud for oil and gas industry. In Proceedings of the International Conference on Signal Processing, Communication, Power and Embedded System, Sankt Goar, Germany, 23–25 May 2016; pp. 1735–1741. [CrossRef]
47. Sivanathan, A.; Gharakheili, H.H.; Loi, F.; Radford, A.; Wijenayake, C.; Vishwanath, A.; Sivaraman, V. Classifying IoT Devices in Smart Environments Using Network Traffic Characteristics. *IEEE Trans. Mob. Comput.* **2019**, *18*, 1745–1759. [CrossRef]
48. Su, J.; Danilo Vasconcellos, V.; Prasad, S.; Daniele, S.; Feng, Y.; Sakurai, K. Lightweight Classification of IoT Malware Based on Image Recognition. *Proc. Int. Comput. Softw. Appl. Conf.* **2018**, *2*, 664–669. [CrossRef]
49. Xiao, L.; Li, Y.; Han, G.; Liu, G.; Zhuang, W. PHY-Layer Spoofing Detection with Reinforcement Learning in Wireless Networks. *IEEE Trans. Veh. Technol.* **2016**, *65*, 10037–10047. [CrossRef]
50. Ahmad, R.; Alsmadi, I. Machine learning approaches to IoT security: A systematic literature review. *Int. Things* **2021**, *14*. [CrossRef]
51. Tahsien, S.M.; Karimipour, H.; Spachos, P. Machine learning based solutions for security of Internet of Things (IoT): A survey. *J. Netw. Comput. Appl.* **2020**, *161*. [CrossRef]
52. Gandhi, U.D.; Kumar, P.M.; Varatharajan, R.; Manogaran, G.; Sundarasekar, R.; Kadu, S. HIoTPOT: Surveillance on IoT Devices against Recent Threats. *Wirel. Pers. Commun.* **2018**, *103*, 1179–1194. [CrossRef]

53. Okpe, O.A. Intrusion Detection in Internet of Things (IoT). *Int. J. Adv. Res. Comput. Sci.* **2018**, *9*, 504–509. [CrossRef]
54. Elrawy, M.F.; Awad, A.I.; Hamed, H.F.A. Intrusion detection systems for IoT-based smart environments: A survey. *J. Cloud Comput.* **2018**, *7*, 1–20. [CrossRef]
55. Yousuf, M.; Parsia, F.; Halder, M. IOT based Automated Intrusion Detection System. *Int. J. Comput. Appl.* **2018**, *180*, 56–61. [CrossRef]
56. Pamukov, M.E.; Poulkov, V.K. Multiple negative selection algorithm: Improving detection error rates in IoT intrusion detection systems. In Proceedings of the 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Bucharest, Romania, 21–23 September 2017.
57. Cervantes, C.; Poplade, D.; Nogueira, M.; Santos, A. Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things. In Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), Ottawa, ON, Canada, 11–15 May 2015; pp. 606–611.
58. Midi, D.; Rullo, A.; Mudgerikar, A.; Bertino, E. Kalis—A System for Knowledge-Driven Adaptable Intrusion Detection for the Internet of Things. In Proceedings of the 37th IEEE International Conference on Distributed Computing Systems(ICDCS 2017) Atlanta, GA, USA, 5–8 June 2017; pp. 656–666.
59. Thanigaivelan, N.K.; Nigussie, E.; Kanth, R.K.; Virtanen, S.; Isoaho, J. Distributed internal anomaly detection system for Internet-of-Things. In Proceedings of the IEEE Consumer Communications and Networking Conference (CCNC 2016), Las Vegas, LV, USA, 8–11 January 2016; pp. 319–320.
60. Karande, J.B.; Joshi, S.A. Comprehensive Assessment of Security Attack Detection Algorithms in Internet of Things. In Proceedings of the 2018 International Conference on Computing Communication Control and Automation. (ICCUBEA 2019), Pimpri-Chinchwad, India, 19–21 September 2019; pp. 1–6. [CrossRef]
61. Hajiheidari, S.; Wakil, K.; Badri, M.; Navimipour, N.J. Intrusion detection systems in the Internet of things: A comprehensive investigation. *Comput. Netw.* **2019**, *160*, 165–191. [CrossRef]
62. Santos, L.; Rabadao, C.; Goncalves, R. Intrusion detection systems in Internet of Things: A literature review. In Proceedings of the 13th Iberian Conference on Information Systems and Technologies (CISTI), Caceres, Spain, 13–16 June 2018; pp. 1–7. [CrossRef]
63. Sforzin, A.; Marmol, F.G.; Conti, M.; Bohli, J.M. RPiDS: Raspberry Pi IDS—A Fruitful Intrusion Detection System for IoT. In Proceedings of the 13th IEEE International Conference on Ubiquitous Intelligence and Computing, Toulouse, France, 18–21 July 2017; pp. 440–448. [CrossRef]
64. Arshad, J.; Azad, M.A.; Salah, K.; Jie, W.; Iqbal, R.; Alazab, M. A Review of Performance, Energy and Privacy of Intrusion Detection Systems for IoT. Available online: https://www.mdpi.com/2079-9292/9/4/629 (accessed on 15 June 2021).
65. Deshmukh-Bhosale, S.; Sonavane, S.S. A Real-Time Intrusion Detection System for Wormhole Attack in the RPL based Internet of Things. *Procedia Manuf.* **2019**, *32*, 840–847. [CrossRef]
66. Zugasti, E.; Iturbe, M.; Garitano, I.; Zurutuza, U. Null is not always empty: Monitoring the null space for field-level anomaly detection in industrial IoT environments. *Glob. Internet Things Summit GIoTS* **2018**. [CrossRef]
67. Da Silva Cardoso, A.M.; Lopes, R.F.; Teles, A.S.; Magalhaes, F.B.V. Real-time DDoS detection based on complex event processing for IoT. In Proceedings of the 3rd ACM/IEEE International Conference on Internet of Things Design and Implementation. (IoTDI 2018), Orlando, FL, USA, 17–20 April 2018; pp. 273–274. [CrossRef]
68. Li, W.; Tug, S.; Meng, W.; Wang, Y. Designing collaborative blockchained signature-based intrusion detection in IoT environments. *Futur. Gener. Comput. Syst.* **2019**, *96*, 481–489. [CrossRef]
69. Laaboudi, Y.; Olivereau, A.; Oualha, N. An intrusion detection and response scheme for CP-ABE-encrypted IoT networks. In Proceedings of the 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS 2019), Canary Island, Spain, 24–26 June 2019; pp. 1–5.
70. Anitha, A.; Revathi, S.; Jeevanantham, S.; Godwin, E.E. Intrusion Detection System based on Artificial Intelligence. *Int. J. Technol.* **2017**, *7*, 20. [CrossRef]
71. Najafabadi, M.M. Machine Learning Algorithms for the Analysis and Detection of Network Attacks. Available online: https://www.proquest.com/openview/f20b71a0184179d51db6c7fae8fb214a/1?pq-origsite=gscholar&cbl=18750 (accessed on 15 July 2021).
72. Othman, S.M.; Ba-Alwi, F.M.; Alsohybe, N.T.; Al-Hashida, A.Y. Intrusion detection model using machine learning algorithm on Big Data environment. *J. Big Data* **2018**, *5*. [CrossRef]
73. Li, P.; Zhang, Y. A Novel Intrusion Detection Method for Internet of Things. In Proceedings of the Chinese Control And Decision Conference (CCDC), Nanchang, China, 3–5 June 2019; pp. 4761–4765.
74. Mo, X.; Chen, P.; Wang, J.; Wang, C. Security and Privacy in New Computing Environments. In *International Conference on Security and Privacy in New Computing Environments (SPNCE)*; Zhou, M., Han, L., Lu, H., Eds.; Springer Nature: Gateway East, Singapore, 2019; Volume 284, pp. 459–471. ISBN 978-3-030-21372-5.
75. Kumar, V.; Das, A.K.; Sinha, D. UIDS: A unified intrusion detection system for IoT environment. *Evol. Intell.* **2019**. [CrossRef]
76. Yang, K.; Ren, J.; Zhu, Y.; Zhang, W. Active Learning for Wireless IoT Intrusion Detection. *IEEE Wirel. Commun.* **2018**, *25*, 19–25. [CrossRef]
77. Hasan, M.; Islam, M.M.; Zarif, M.I.I.; Hashem, M.M.A. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. *Int. Things* **2019**, *7*, 100059. [CrossRef]

78. Chaabouni, N.; Mosbah, M.; Zemmari, A.; Sauvignac, C.; Faruki, P. Network Intrusion Detection for IoT Security Based on Learning Techniques. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2671–2701. [CrossRef]
79. Deng, L.; Li, D.; Yao, X.; Cox, D.; Wang, H. Mobile network intrusion detection for IoT system based on transfer learning algorithm. *Cluster Comput.* **2018**, 1–16. [CrossRef]
80. Girnar, N.; Kaur, S. Intrusion detection for Adhoc networks in IOT. In Proceedings of the International Conference on Intelligent Computing and Control Systems (ICICCS 2017), Madurai, India, 15–16 June 2017; pp. 110–114. [CrossRef]
81. Anthi, E.; Williams, L.; Slowinska, M.; Theodorakopoulos, G.; Burnap, P. A Supervised Intrusion Detection System for Smart Home IoT Devices. *IEEE Internet Things J.* **2019**, *6*, 1. [CrossRef]
82. Nivaashini, M.; Thangaraj, P. A framework of novel feature set extraction based intrusion detection system for internet of things using hybrid machine learning algorithms. In Proceedings of the International Conference on Computing, Power and Communication Technologies (GUCON 2019), Greater Noida, India, 28–29 September 2018; pp. 44–49.
83. Shukla, P. ML-IDS: A machine learning approach to detect wormhole attacks in Internet of Things. In Proceedings of the SAI Intelligent Systems Conference (IntelliSys 2017), London, UK, 7–8 September 2017; pp. 234–240. [CrossRef]
84. Ioannou, C.; Vassiliou, V. Classifying Security Attacks in IoT Networks Using Supervised Learning. In Proceedings of the 15th International Conference on Distributed Computing in Sensor Systems, Santorini Island, Greece, 29–31 May 2019; pp. 652–658. [CrossRef]
85. Bakhtiar, F.A.; Pramukantoro, E.S.; Nihri, H. A Lightweight IDS Based on J48 Algorithm for Detecting DoS Attacks on IoT Middleware. In Proceedings of the the 2019 IEEE 1st Global Conference on Life Sciences and Technologies (LifeTech 2019), Osaka, Japan, 12–14 March 2019; pp. 41–42. [CrossRef]
86. Zhao, S.; Li, W.; Zia, T.; Zomaya, A.Y. A dimension reduction model and classifier for anomaly-based intrusion detection in internet of things. In Proceedings of the 2017 IEEE 15th International Conference on Dependable, Autonomic and Secure Computing, 15th International Conference on Pervasive Intelligence and Computing, 3rd International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech 2017), Orlando, FL, USA, 6–10 November 2017; pp. 836–843.
87. Cvitic, I.; Perakovic, D.; Gupta, B.; Choo, K.K.R. Boosting-based DDoS Detection in Internet of Things Systems. *IEEE Internet Things J.* **2021**. [CrossRef]
88. Hamza, A.; Gharakheili, H.H.; Benson, T.A.; Sivaraman, V. Detecting Volumetric Attacks on IoT Devices via SDN-Based Monitoring of MUD Activity. In Proceedings of the 2019 ACM Symposium on SDN Research (SOSR. 2019), San Jose, CA, USA, 3–4 April 2019; pp. 36–48. [CrossRef]
89. Sivanathan, A.; Gharakheili, H.H.; Sivaraman, V. Detecting Behavioral Change of IoT Devices Using Clustering-Based Network Traffic Modeling. *IEEE Internet Things J.* **2020**, *7*, 7295–7309. [CrossRef]
90. Cvitić, I.; Peraković, D.; Periša, M.; Botica, M. Novel approach for detection of IoT generated DDoS traffic. *Wirel. Netw.* **2021**, *27*, 1573–1586. [CrossRef]
91. Vengatesan, K.; Kumar, A.; Naik, R.; Verma, D.K. Anomaly based novel intrusion detection system for network traffic reduction. In Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud (I-SMAC 2019), Tamil Nadu, India, 12–14 December 2019; pp. 688–690. [CrossRef]
92. Zhang, Y.; Li, P.; Wang, X. Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network. *IEEE Access* **2019**, *7*, 31711–31722. [CrossRef]
93. Diro, A.A.; Chilamkurti, N. Distributed attack detection scheme using deep learning approach for Internet of Things. *Futur. Gener. Comput. Syst.* **2018**, *82*, 761–768. [CrossRef]
94. Shenfield, A.; Day, D.; Ayesh, A. Intelligent intrusion detection systems using artificial neural networks. *ICT Express* **2018**, *4*, 95–99. [CrossRef]
95. Aslan, Ö.; Samet, R. A Comprehensive Review on Malware Detection Approaches. *IEEE Access* **2020**, *8*, 6249–6271. [CrossRef]
96. Xiao, F.; Lin, Z.; Sun, Y.; Ma, Y. Malware Detection Based on Deep Learning of Behavior Graphs. *Math. Probl. Eng.* **2019**, *2019*. [CrossRef]
97. HaddadPajouh, H.; Dehghantanha, A.; Khayami, R.; Choo, K.K.R. A deep Recurrent Neural Network based approach for Internet of Things malware threat hunting. *Futur. Gener. Comput. Syst.* **2018**, *85*, 88–96. [CrossRef]
98. Yuxin, D.; Siyi, Z. Malware detection based on deep learning algorithm. *Neural Comput. Appl.* **2019**, *31*, 461–472. [CrossRef]
99. Cui, Z.; Xue, F.; Cai, X.; Cao, Y.; Wang, G.G.; Chen, J. Detection of Malicious Code Variants Based on Deep Learning. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3187–3196. [CrossRef]
100. Hashemi, H.; Azmoodeh, A.; Hamzeh, A.; Hashemi, S. Graph embedding as a new approach for unknown malware detection. *J. Comput. Virol. Hacking Tech.* **2017**, *13*, 153–166. [CrossRef]
101. AL-Hawawreh, M.; Moustafa, N.; Sitnikova, E. Identification of malicious activities in industrial internet of things based on deep learning models. *J. Inf. Secur. Appl.* **2018**, *41*, 1–11. [CrossRef]
102. Kim, J.Y.; Bu, S.J.; Cho, S.B. Zero-day malware detection using transferred generative adversarial networks based on deep autoencoders. *Inf. Sci.* **2018**, *460–461*, 83–102. [CrossRef]
103. Azmoodeh, A.; Dehghantanha, A.; Conti, M.; Choo, K.K.R. Detecting crypto-ransomware in IoT networks based on energy consumption footprint. *J. Ambient Intell. Humaniz. Comput.* **2018**, *9*, 1141–1152. [CrossRef]

104. Doshi, R.; Apthorpe, N.; Feamster, N. Machine learning DDoS detection for consumer internet of things devices. In Proceedings of the 2018 IEEE Symp. Secur. Priv. Work (SPW 2018, 29–35), San Francisco, CA, USA, 24 May 2018. [CrossRef]
105. Agrawal, R.; Stokes, J.W.; Selvaraj, K.; Marinescu, M. Attention in Recurrent Neural Networks for Ransomware Detection. In Proceedings of the 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2019), Brighton, UK, 17 May 2019; pp. 3222–3226. [CrossRef]
106. Yuan, Z.; Lu, Y.; Xue, Y. Droiddetector: Android malware characterization and detection using deep learning. *Tsinghua Sci. Technol.* **2016**, *21*, 114–123. [CrossRef]
107. Vinayakumar, R.; Alazab, M.; Soman, K.P.; Poornachandran, P.; Venkatraman, S. Robust Intelligent Malware Detection Using Deep Learning. *IEEE Access* **2019**, *7*, 46717–46738. [CrossRef]
108. Adamu, U.; Awan, I. Ransomware prediction using supervised learning algorithms. In Proceedings of the 7th International Conference on Future Internet of Things and Cloud (FiCloud 2019), Istanbul, Turkey, 26–28 August 2019; pp. 57–63. [CrossRef]
109. Adebayo, O.S.; Aziz, N.A. Improved Malware Detection Model with Apriori Association Rule and Particle Swarm Optimization. *Secur. Commun. Netw.* **2019**, *2019*. [CrossRef]
110. Rhode, M.; Burnap, P.; Jones, K. Early-stage malware prediction using recurrent neural networks. *Comput. Secur.* **2018**, *77*, 578–594. [CrossRef]
111. Villanueva, J.A.; Juanatas, R.; Lacatan, L.L. Malware predictor using machine learning techniques. *Test Eng. Manag.* **2020**, *82*, 5665–5674.
112. Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J. Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges. Available online: https://link.springer.com/article/10.1186/s42400-019-0038-7. (accessed on 19 July 2021).