[1] Sarika

2 Rajeshwar Dass

# Investigation of Machine Learning-based Software Definition Network for Intrusion Detection in IoT

JES
Journal of Electrical Systems

***Abstract: -*** The World Wide Web of Things will impact many aspects of our lives. Home automation gadgets, sensors, and garments use it. Internet of Things devices shine out for connectivity, wide use, and cheap computing power. By 2024, 50 billion items will be connected to the Web as gadgets for the Internet of Things develop increasingly prevalent. IoT-enabled software-defined networks manage large amounts of unpredictable internet traffic. However, huge internet traffic makes it hard to identify fraudulent activity. IoT device safety investigations are best done with machine learning and deep learning. SDN-based IoT vulnerability protocols, architecture, and dangers are the focus of this study. Intrusion detection methods are listed below. The investigation also examines machine learning and deep learning strategies for detecting Internet of Things gadgets at risk of infiltration.

***Keywords:*** software-defined network security; software-defined network protocols; intrusion detection system; machine learning; deep learning;cyber-attacks

## 1.0.Introduction

IoT and other telecommunications and technological innovations have outpaced traditional detection methods. The World Wide Web of Things makes initiatives to enhance living circumstances possible. ‘The fastest-growing computer sector group, the Internet of Things (IoT), is expected to have 50 billion connected devices by 2020. We expect IoT and associated technologies to generate $3.9 trillion to $11.1 trillion annually by 2025 [1]. Web of Things innovations including embedded gadgets, ubiquitous and omnipresent computing, connected sensors, Web standards, and apps powered by AI may make IoT devices intelligent [2]. Since they are interconnected, IoT gadgets may communicate and calculate like their distributed counterparts [3]. These gadgets can automatically collect current information from authentic products due to their various sensors. Internet-connected physical devices pose safety risks [4,5]. Smart safety measures are needed to safeguard IoT devices from harmful traffic. As the IoT expands, novel safety precautions must be implemented to secure devices as well as information [6, 7]. When unchecked, attackers enter IoT devices and commit crimes [8,9]. IoT devices commonly use internet connections, therefore eavesdropping may reveal confidential data [10,11]. IoT gadgets lack the energy and computing power to add security solutions to these issues. IoT connectivity and integration have created new threat surfaces [12,13]. Thus, IoT systems are more susceptible than previous computers. SDN needs explicit research and preventive procedures to thwart attacks on SDN-based devices. Software-defined network systems need a second cyberdefense layer. This may be done with IDSs [14,15]. Many studies have used machine learning to classify IDSs to battle software-defined IoT networks. assessments include ad hoc networks that are portable, wireless sensors, cloud-based software-defined network security systems, and cyber-physical system assessments [16,17].

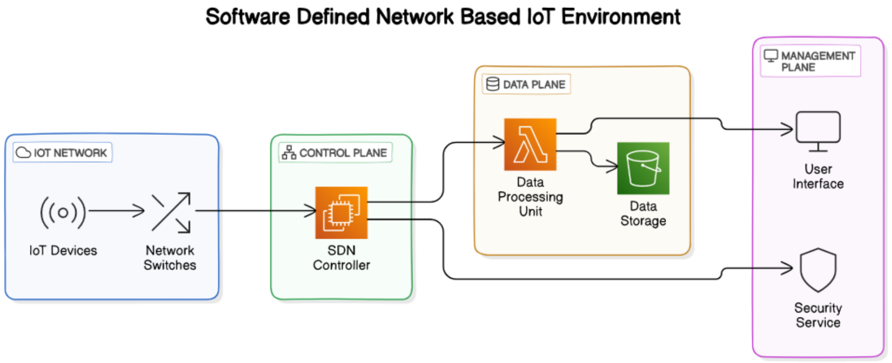

**Fig.1** Software-Defined Network based IoT environment

Software-defined network infrastructures are less safe utilising typical IDS approaches because to their pervasiveness, heterogeneity, finite bandwidth capacity, and global connectivity. Machine learning (ML) and deep

[1] Research Scholar, ECED, DCRUST, Murthal, Sonipat (HR), India. sarikasoni006@gmail.com

[2] Associate Professor, ECED, DCRUST, Murthal, Sonipat (HR), India. rajeshwardas10@gmail.com

learning (DL) methods for network assault detection are becoming more popular. Software-defined network systems may identify normal and pathological activity via ML/DL. Analyzing communication between networks and IoT gadgets might reveal trends. These established trends can help detect abnormal conduct. ML/DL-based methods have also been investigated for predicting zero-day attacks. ML/DL algorithms enable reliable security for SDN networks and their components. Most software-defined network (SDN) scientists haven't considered employing deep learning or machine learning to construct an IDS for IoT systems. According to [18,19], this research analyzed software-defined network security issues and classified them by implementation, system, authentication and identification, and access constraints. This paper evaluates ML and DL-based IDS in software-defined networks and identifies research needs.

***Scope of this survey***

This paper covers IDS architectures and designs, ML/DL methods used in design, datasets for evaluation, future research challenges, and specific suggestions. Six components make up this paper.

***Main Contribution***

This article examines how machine learning and deep learning recognise IoT, T network, and connected device assaults and network threats. Table 1 compares traditional networking to software-defined networking—ML and DL-based IDS approaches for networks and systems. Results of the study:

- Analysed IoT protocols and designs, including available technologies, radio frequency ranges, and data speeds.
- A key standard for identifying IoT vulnerabilities, threat environments, attack surfaces, and relevant attack types for protocols.
- An in-depth analysis of IDS pros and cons using ML and DL. Network and software-defined network security datasets must be carefully assessed for pros and cons.
- Explain the development of software-defined networks and systems employing IDSs using ML and DL approaches, including current research areas and future goals.

## 2. Current Reviews

Software-defined network security audits have shown flaws in the systems. However, recent research on software-defined network security has not paid much attention to how well ML/DL techniques may be utilized to safeguard these networks. The authors of [20] investigated IoT devices' communication layer security problems. [21] conducted a study on the assessment of IDSs for SDNs. [22] describes the machine learning research on software-defined network safety and confidentiality. They also noted that IoT lacks storage, computational capacity, and bandwidth for ML-based security solutions. Much research has used ML along with data analysis methods to locate irregularities or categories of traffic in software-defined network networks to detect intrusions [23]. The authors of [24] say software-defined networks vary from wired networks in various respects. Due to the architectural quirks of the World Wide Web of Things and AI, IDSs, hazards, fundamental technologies (interactions and infrastructure), and the programmed level must be considered.

Another research [25] focused on the use of IDS in a mobile ad hoc network (MANET) setting. The authors looked at the three most valuable IDS design types for MANETs. A hierarchically tiered system with tiers might be the first option. On the other hand, a different deployment architecture could be appropriate in a distributed, collaborative setting. The two are combined as a result of mobile agents. Another study [26] examined several IDS implementations in intrusion detection methods connected to MANET. The authors suggest that various IDS approaches may be categorized based on the underlying theory employed for attack detection. For example, one may use rules, statistical data, heuristics, requirements, a signature, a reputation score, or an application strategy to explain these notions to others. Abuse methods, hybrid, hybrid-based, and anomaly detection approaches were the following four divisions from such methodologies. The authors [27] also offer real-time/offline, attack kind, and detection efficacy as additional classification criteria (scalability, reliability, timeliness, etc.).

Numerous studies have categorized IDS for Wireless Sensor Networks(WSN) according to how IDS agents are deployed [28]. Establishing WSNs is advised to utilize a hybrid deployment approach incorporating both central and decentralized deployment advantages. WSNs were categorized using IDS detection-type criteria in a similar experiment [29]. Requirement-based detection was one of the classes discovered. These cloud-based IDSs, according to the authors of [30], have an impact on security, accessibility, and authenticity. (CIA) of software-defined networks built on cloud computing. A variety of IDS tactics, including distributed, networked, and hypervisor-based ones, were covered in the debate. When describing IDS for SDNs, the IDS architecture was emphasized in [31]. The survey's conclusions included IoT protocols, standards, technologies, and security issues[32-36].

### 2.1 software-defined networks(SDN)

The information and command planes of the World Wide Web of Things are divided by a novel networking design called "software-defined networking. For example, an SDN switch features flow tables that a software program may handle differently than a regular switch. Since its architecture is based on several well-known principles, SDN isn't new. Research tracks, publications, trends, and other factors were considered during a systematic literature review (SLR) of the existing literature. In light of this, we conduct in-depth evaluations of IoT research. Internet of Things (IoT) technologies, research fields, security concerns, and opportunities are all discussed in the report (IoT). A technique for designing networks is 'Software Defined Networking.' It enables software-based network management and control. Using open APIs in software applications, the Software Defined Network provides centralized programming for the whole network and its constituent parts. An IoT relies on software-controlled apps or APIs to operate the entire network, and network virtualization boosts IoT performance. These programs and APIs may interact with the underlying hardware or regulate network activities. It appears that software-defined networking, which enables connections to function or construct virtual equivalents, is what the World Wide Web of Things (IoT) is all about.

**2.2 Comparison of software-defined networks and traditional networks**

| S.No. | SDN | TRADITIONAL NETWORK |
|---|---|---|
| **01.** | A software-defined network is a distributed networking technique. | The conventional system uses antiquated communication methods. |
| **02.** | distributed networking technique. | A conventional system is described as decentralized control. |
| **03.** | Software Defined Network is about centralized management. | Programming this network is not possible. |
| **04.** | It is possible to customize this network's configuration. | A conventional system has a closed interface. |
| **05.** | Both the control plane and the data plane of a networking system are divided inside software by defined software. | Data and control planes are installed on the same plane in conventional networks. |
| **06.** | It allows for an automated setup, which cuts down on time. | It requires more time since it offers static/manual configuration. |
| **07.** | Certain network packets may be prioritized and blocked. | All packets are led in the same direction without provision for prioritizing. |
| **08.** | It's simple for the programmer to meet your needs. | It is challenging to replace outdated programmers with new, more useful ones. |
| **09.** | The cost of Software Defined Networks is low. | Conventional Networks Are Pricey. |
| **10.** | The underlying architecture of the Software Defined Network is straightforward. | The structure of a conventional network is rather complicated. |
| **11.** | A software-defined network has a great degree of adaptability. | Conventional networks have limited adaptability. |
| **12.** | SDN simplifies monitoring and debugging since it is controlled and centralized. | A typical network's dispersed control makes monitoring and debugging difficult. |
| **13.** | They have lower costs for upkeep than traditional networks. | Conventional network maintenance costs are higher than those of SDN. |

**2.3 challenges in software-defined networks:**

When a system fails, users must be notified, and a remedy must be made swiftly. Reliability is essential. The code's dependability must be considered when developing high-quality software. Reliability in software refers to the possibility that a program will function as anticipated over time and in a given set of circumstances. To improve network availability, allow problem treatment and prevention, and enable these activities, the N controller must be intelligently set up and verify network management. Although [4], a production-grade SDN controller, had a few difficulties, the authors concluded that problem count, detection, and resolution time behaviour were mainly consistent over versions. Flow control and continuity are maintained if a network component breaks or malfunctions. Thus, traffic is redirected to neighbouring channels or nodes. A single controller manages the whole network in SDN; if this controller goes down, the network might disappear. To increase network stability, software providers and developers should fully use controller functions.

An SDN controller should be able to handle 100 switches effortlessly. However, flow table entries and network broadcast overhead must also be considered drawbacks. The ability of a system, network, or process to accommodate an increase in workload or capacity is referred to as 'system scalability.'.

Low-level interface: The SDN framework must transform these network rules into low-level switch configurations. For SDN networks, control applications should be able to define network rules. Even the simplest operations need the SDN framework's programming interface to manage the many asynchronous events at the switches.

Efficiency and safety: Depending on how it is constructed, the SDN network may be more susceptible to different new sorts of network assaults, which would reduce the SDN's total value. The authors quickly examine a variety of security concerns and obstacles before discussing cloud computing security. The possibility of several DDoS strikes rendering networks worthless exists. One of the topics mentioned by either author is SYN. Flood assault can shut down any organization's server by flooding the TCP queue. Applications integrity, centralized control, network risk identification and prevention, user identification and permission must all be integrated into SDN platform solutions.

### 2.4 Attacks on software-defined networks

The network manipulation seems to be a severe attack on the control plane. False network data is generated along with other assaults on the whole network when the IoT controller is taken over.

Changing transportation routes: This attack targets network components at the data plane level. Eavesdropping is made feasible by the attack's usage of a network device.

Utilize a side channel to attack: This attack targets components of the data plane network. The assault makes use of a network device, making eavesdropping possible. Additionally, this attack involves the manipulation of the application plane. Programming errors might lead to data eavesdropping or service interruptions. A criminal might use this to access an IoT application and conduct crimes.

DoS attack: The most frequent assault against the SDN is a denial of service (or ‘DoS’) attack, which can potentially halt the whole network. For example, a DoS attack by an adversary might deactivate or limit all SDN capabilities.

ARP (Address Resolution Protocol) fraud, commonly referred to as ARP cache ingestion, is used in a man-in-the-middle assault. All these activities are conceivable when an attacker uses ARP spoofing to gain access to the network. Traffic monitoring, modification, and even blocking, such assaults contaminate both network data and topology-aware SDN applications. A hacker could get confidential data without the owner's permission by exploiting API(Application Programmable Interface) flaws. Additionally, due to API misuse, network traffic may be disrupted on the northbound interface.

Sniffer attack: Hackers often use sniffer attacks to gather and analyze data on network connectivity. Hackers may access private information via monitoring network connections or other systems. Any situation with a reliable supply of air is conducive to sniffing. For example, an IoT hacker may use unencrypted communications to track traffic to and from a central controller. The information learned here could help determine how the network works or what traffic is allowed. It is possible to perform a password guessing or brute force attack to target non-IoT components. For example, an unauthorized party might breach the Internet of Things via brute force or password guessing.

### 2.5 Application of Software-Defined Networks

An SDN application is software created specifically for use with software-defined networking. A typical network's hardware components' firmware may be replaced or enhanced by SDN applications. Various SDN architectures are available. Here is an illustration of an architecture using SDN controllers. All the hardware and cables needed to support a network are housed in the physical infrastructure layer of the SDN architecture. SDN controllers take over network management when the hardware is no longer considered. The second layer of the architecture consists of the controllers in charge of starting and stopping traffic. Applications running on SDN servers, or software-defined networks, make up the third layer. These programs route specific tasks using the controller. SDN applications include network virtualization, monitoring, intrusion detection, and traffic balancing.

## 3. IoT System Environment

The World Wide Web of Things is widely used in real-world applications including commercial, regional, and household automation. As a result, several microprocessors and resource-saving transmission norms, procedures, and innovations are currently being developed. Various sectors make use of these systems. The common ones include business, education, agriculture, and the military. gadgets guidelines and guidelines for communication have evolved as a result of investigations in several application domains. To offer smart solutions to customers, the Internet of Things (IoT) architecture links physical items with computer systems and networks of communication. The Internet of Things requires flexible, tier-based architecture to link billions of sensors. Even though multiple researchers and organizations have produced several designs and standards [37, 38], no one model is universally recognized. In this compilation of well-known designs, the terms "design" and "reference model" are employed interchangeably[39, 40]. The senses layer—also referred to as the "device layer"—is an extremely widely used and important design that includes real hardware and devices. It has network and communication tiers in addition to application and sensory layers. The sensor data collected through telemetry had to be safely sent to the networks for analysis and interpretation by the network layer, also known as the "transmission layer"[41, 42]. According to the International Telecommunication Union (ITU), an IoT reference architecture has been created, enabling global management of applications using network layer technology[43,44]. The Internet of Things should be separated into four layers, with management or security components connecting each layer to the next. [45] Here is a list of the levels: An architecture comprises the following layers: application, device, network, service support, and service. The European Commission suggests the architectural reference model (IoT-A). Martin Bauer and colleagues created IoT-A, which the European Commission funded as a component of FP7(Seventh Framework Programme). [46]

### 3.1 SDN-based IoT environment:

communication activities (SD-GWs), the software offers SDN and cross-layer tuning for novel IoT gadgets and radio-based systems. To overcome these challenges, a mix of 5G and IoT networks has been created in response to the spike in the number of gadgets that are connected. Mobile Network Optimization Using SDN: When real radio frequency intervention is required, achieving the desired result in a congested communications environment is far more difficult. In the framework of SDN routed networks (SDN), EPA (Ethernet for Plant Automation) and RNOPA (Ranking-based near-optimal Placement Algorithm) have been suggested as potential remedies for the decline in cloudlets at the same location with different APs in the Internet of Things (IoT). For IoT connection operations (SD-GWs), the software offers SDN and cross-layer optimization for novel IoT electrical gadgets and radio-based platforms. To overcome these challenges, a mix of 5G and IoT systems has been created in response to the spike in the number of connected devices.

IoT devices with SDN and wireless sensors**:** In the IoT ecosystem, wireless sensors must be more scalable and energy-efficient. Numerous SDN-based initiatives have previously been identified in the literature to accomplish this. An SDN-based solution was developed to address the issues raised by low-power Wi-Fi networks. The WSN infrastructure built on the SDN architecture is ready to operate in cloud computing environments. IoT management problems, including fault tolerance, dependability, control flow control, and mobility across diverse and congested networks, to mention a few, may benefit from SDN. However, UbiFlow claims that segmenting the urban-scale SDN requires many controllers. The ‘Trust List’ explains how trust is dispersed across IoT-related parties and how SDN and blockchain should be correctly coupled to implement control of information at the network's periphery.

IoT Security Framework for SDN: Consumers may run across security concerns like malware attacks and unauthorized user access while using the internet. IoT gadgets are causing new security threats and flaws. Edge servers may activate security authentication after completing a basic authentication process. An also used SDN and blockchain technologies to eliminate the need for re-authentication. The architecture of the IoT network is further protected by granular rules that allow networking-based device authentication for IoT devices.

Applications of SDN-Based IoT in Smart Cities: SDN has dependability difficulties, but the system has been hit worst by one of them. SDN divides the data and control planes to boost network design flexibility. SDN-IIoT, which manages server load, is an example of a QoS-aware architecture.

### 3.2 IoT-Based Threats and Attacks

IoT systems are now more vulnerable to security flaws than traditional computer systems [49,50]. First, there are many different tools, platforms, protocols, and methodologies used by Internet of Things (IoT) systems to communicate data. Second, while control devices were employed to connect physical systems. Third, since people and items are constantly moving, IoT systems are dynamic and lack fixed boundaries[51,52]. On the other hand, specific IoT solutions can pose a health risk. Due to their low energy capacity, IoT devices may be challenging to implement contemporary security processes and technologies. Nodes in IoT networks may evaluate noise, temperature, and light levels before adjusting HVAC controls. These nodes might number in the hundreds in an IoT network. These sensors and control systems may communicate with one another using a variety of network protocols, including Bluetooth, WiFi, ZigBee, and others[53]. Standards, services, and technologies at every level of the IoT ecosystem raise data security and privacy concerns. Although it may seem that security issues in IoT environments are comparable to those in the cloud, mobile, and other communication networks, IoT settings are distinct owing to a few features and innovative security processes used in IoT[54,55]. They may use a few computer resources to connect to many IoT devices and send data to and from them.

The September 2016 620 Gbps attack on Brian Krebs' security blog was the result of an IoT malware built by the Mirai malware, making IoT devices vulnerable. It's possible that this assault used the biggest botnet size ever. To get access to network-enabled cameras, home routers, and digital video recorders—devices with fewer security measures than other Internet of Things devices—Mirai utilised a straightforward method that scanned an inventory of 62 frequently used login information[56,57]. The largest DDoS assault was launched using Mirai against the French web hosting provider on VousHéberge, and it peaked at 1.1 Tbps [58]. The too-lenient default security settings made it feasible. Because of implementation problems in protocols, the authors showed how easy it is to attack different types of Internet of Things gadgets [59]. "The chance of unwanted exposure of personally identifiable information on these systems will increase as the growing amount of Internet of Things, or IoT, gadgets increases. With the use of detectors and other readily accessible IoT devices, the researchers of [60] found several security flaws in networks made up of IoT devices.

One example is an intelligent irrigation system that monitors environmental variables like humidity and temperature. The web-based user interface was functioning thanks to the actuator module. The system was constructed using an Arduino Uno. While the SoftAP(Software Application) was broadcasting packets that reauthenticated IoT devices, an attacker could temporarily disable any IoT device on the network, leaving the network vulnerable to spoofing. Because the SoftAP appeared to have a more powerful signal compared to a real access point (AP) with an identical function set identities, the hacker was able to join Internet of Things ( IoT ) gadgets to the system as a result[61,62].

Consequently, all network communications are at risk from listening devices and man-in-the-middle assaults. IoT networks may use IDSs to identify IoT device vulnerabilities caused by different attack scenarios. ‘The World Wide Web's underlying concept is that communication may be made more accessible by intelligently linking the physical world to the internet[63,64]. IoT ecosystems are thus interconnected and reliant on a range of outside factors. Because of this, every IoT system has to be on high alert for cyberattacks originating from all possible angles[65,66]. Both physical and virtual attacks against IoT systems are possible. Even though our study primarily focuses on cyber threats, which may be active or passive assaults, IoT Security hazards may be broadly separated into the physical and cyber worlds. Since passive attacks do not affect the flow of information, they damage the privacy and confidentiality of dialogue[67,68]. For example, IoT device location monitoring may sometimes be enabled via a passive attack. During active assaults, various information and data flows, such as device settings, control messages, and software components, are continuously updated and modified. For example, a sizeable DDoS assault on the Internet was recently carried out using an IoT device. IoT devices are attractive targets for these attacks owing to their widespread usage and relatively easy entry due to lax security standards and inadequate defences[69]. For example, IoT devices may be compromised by the Mirai botnet attack. [70,71] IoT systems must protect themselves against several attack vectors, including The consumer interface, internet connectivity, internet services, and additional linked IoT gadgets with sensors[72].

***UserInterface***

Most IoT system use cases include offering services to clients using equipment with an application's graphical interface (the internet, the computer, or smartphone). Customers may control innovative home technologies using mobile apps. Due to the growing popularity of smartphones, malicious software and malware may now be concealed inside applications and marketed as useful mobile apps [73,74]. Platform flaws, like those in Android that were recently discovered, might provide hackers access to mobile devices. Malware might thus infect the phone and get access to all of its data. User interface technology may be exploited for DoS or DDoS generation, bluejacking, and bluesnarfing, in addition to listening in on conversations and watching users' movements [75,76].

***cloud services***

IoT devices and cloud services might come together to produce a fantastic technological mashup despite being at different extremes of the technology spectrum. Cloud services' access to computation, storage, and other resources may compensate for IoT device limitations [77]. Utilising IoT gadgets to their full capacity is feasible and cloud services for energy savings and service delivery without restrictions on storage and processing capability [78,79]. For cloud services with extensive IoT system installations, including apps may be helpful [80]. As we'll see in a moment, a dispersed setup like this allows for several entry points at different phases of an attack.

By taking advantage of weaknesses in data security laws, an attacker may get unauthorized access to cloud and IoT systems. Infractions of morality. Attackers may quickly access databases while jeopardizing the data's accuracy using spoofing and other methods—an unreliable visualization system. An attacker may take advantage of a weakness in the virtualization platform to get beyond the security and isolation barriers separating the host OS(Operating System) from the guest OS. This security issue could cause the trend of assaults and privilege escalation to reverse. [81]. Encroachment of private space data about the patient's health may be monitored via IoT solutions, such as wearable technology. Smart home gadgets likewise monitor the user's confidential information. Regarding privacy and secrecy, cloud services' drawbacks exceed their advantages. Additionally, the multi-tenancy of cloud services, with their widespread reach, puts data security at risk owing to Malware and growing privileges [82, 83].

***Links between several IoT systems***

Smart homes and cars are now all equipped with sensors and actuators that operate autonomously and communicate with one another without the need for a human user, in addition to other WoT devices. Smart buildings and vehicles can interact and perform related activities. [84] gave the case where an intelligent plug was disconnected while a temperature sensor detected an increase in temperature, resulting in the windows opening on their own, an example. An attacker might degrade the actuator by tampering with the temperature sensor device [85,86]. This linked Internet of Things system includes vulnerabilities that put other components at risk, as seen in the picture below. Millions of additional devices might be affected by a single hacked device, increasing the possibility of every attempt succeeding and the damage. All systems and networks connected face the danger of being hampered. Even if legitimate cryptographic authentication measures are in place to prevent malicious firmware updates, a malware experiment targeting Philips Hue intelligent lights has compromised every bulb in the network [87,88]. Similar tactics may prevent DDoS attacks against external targets or control over city lights [89,90]. IoT systems need sensors like IP cameras, RFID, GPS, and temperature gauges. Sensors and actuators are used by autonomous automobiles as well as the Internet of Cars (IoC). They are vulnerable to physical harm and exploitation by criminals. The actuator, which executes a function based on sensor data, is another element of WoT devices vulnerable to assaults. In DoS attacks, actuators and sensors target flooding, eavesdropping, tracking, and spoofing techniques[91,92].

***Radio-Frequency Identification(RFID)***

Since RFID devices communicate over an open wireless link, unauthorized readers could access the data. RFID technologies seem less secure than conventional wireless networks [75]. Currently, the following RFID hacking techniques are being discussed: Remove the tag if it's still attached. In addition to sending a death signal, a tag attacker can also deactivate a title if the antenna is destroyed and the memory is purged.

Tag modifications*:* The attacker modifies or deletes the tag's memory. After scanning the victim's data, an attacker copies the tags using labels and then duplicates or fabricates the tags.

Reverse Engineering: Reverse engineering is a technique that may be used to duplicate and analyze a tag to extract any confidential information it could contain.

Maintaining a journal: Ultra-high frequency (UHF) RFID systems are more susceptible. An attacker could read data sent between a real reader and an actual tag.

Scuba diving: The attacker places an unauthorized reader within the tag so they may also interact with it. Unauthorized readers and tags send scanner data that may be intercepted.

Another assault: The attacker listens in on the WoT gadget to gather details since the goal of an attack is to mislead.

Relay-based attacks include the unauthorised placement of the gadget among the label and the viewer. This device is used by an intruder to quickly capture, alter, and transmit information with other devices.

Electromagnetic field interference (EM): An attacker sends a signal near the reader to interact with readers to avoid tagging.

Using a phoney RFID tag to search: An attacker sends an identical request to several titles to locate a specific tag.

Algorithm decryption attacks: After violent attacks have rendered encryption systems useless, the plain text may still be retrieved by decoding the intercepted cryptography attacks by tagging a blocker. An attacker may use a blocker tag to prevent the reader from accessing tags.

***ZigbeeProtocol***

IoT devices rapidly use the Zigbee protocol because of its cheap cost, scalability, and low power consumption. Zigbee was created with security in mind, but compromises were needed to decrease gadget costs while simultaneously boosting their scalability. Failure to follow proper security practices eventually led to security vulnerabilities. The following is a list of the significant security threats to Zigbee networks. It has a strange quality about it. Since there is no encryption in Zigbee, networks are susceptible to sniffing attacks. Attackers may use software tools like KillerBess' Zigbee program [93] to capture certain packets and use them for evil purposes. Repetition is a powerful instrument in the assault. It may be rebroadcast as ordinary traffic if the hacker successfully obtains the network data [94].

Having the Link key or the Network key, an attacker may access the ZigBee network's connection keys since they must be restored over the air each time one of the network's ZigBee devices is flashed. In addition, users may physically take keys from a ZigBee device's flash memory by gaining access to it[95,96]. A MiTM (Man-in-the-Middle attack) attack has the potential to divert and eavesdrop on communication on a ZigBee network. Launch an assault by destroying ZED(Zigbee End-Device). The ZED assault was suggested by the ZigBee protocol's creators [97] as both an offensive and defensive tactic (ZED). The assault aims to deactivate the ZED by sending out a specific signal that will awaken it and drain its charge. In Wireless Fidelity (WiFi) [80], a thorough explanation of attacks against 802.11 security mechanisms is provided. WPA2( Wi-Fi Protected Access Wireless Security Protocol) is the ancestor of WPA (Wireless Application Protocol) and WPA2. The most common WiFi attacks are thoroughly described in the next section.

In attacks Associated with Key Recovery, an attacker would keep an eye on a small number of certain packets to do offline key cracking. The acronyms Pushkin, Tews, and Weinmann (PTW), Fluhrer, Mantin, and Shamir (FMS), Korea Family, Dictionary, and address resolution protocol (ARP) Injection are often used to refer to attacks in this field [98,99]. • An effort at Keystream Recovery. The only thing an attacker needed to do before doing the offline key cracking was to keep an eye out for certain packets. PTW assaults, FMS assaults, Korea Family assaults, Dictionary assaults, and ARP Injections are the most frequent attacks in this category [80]. Attacks on DoS or accessibility These assaults are referred to as ‘DoS’ attacks because they prevent service or network from being accessed. To lower network efficiency for every individual, such assaults frequently focus on one user or equipment and deplete the reserve of resources (which might include the network switch or Gateway Point). Due to the open nature of 802.11 management messages up to 802.11n and the ease with which forged versions of these messages may be broadcast, these attacks are straightforward to execute. The Beacon Flood, Probe Request and Response, Fake Power Saving, Authentication Request Flood, Block ACK Flood, de-authentication Broadcast(DB), and Disassociation Attack(DA). Some examples of this kind of assault include Flood Assaults(FA). Denial-of-Service (DoS) attacks against 802.11 are described in detail [100].

***Bluetooth***

Most issues arise at the Bluetooth connection stage. Attacks might begin before or after the devices are linked, among other times [83]. Attackers might use the information they learned via pairing to perform such as man-in-the-middle assaults. [101] provides an outline of Bluetooth safety concerns. This section gives a summary of some of the typical Bluetooth attacks. Trying to figure out a PIN: Attackers use this method when trying to pair and authenticate devices. An attacker might use a frequency sniffer application to retrieve the Bluetooth Device Address (BD ADDR) and a random number from the targeted device (RAND). After the correct PIN has been found, To verify every potential PIN conjunction, a brute-force method (like the E22 method) is employed [102].
A MAC spoofing assault: An attack occurs when link keys are produced before encryption. Devices may authenticate one another using created link keys. As a consequence, attackers may fake many users. In addition, cybercriminals may change data, and connections can even be destroyed [103].
Assaults by MIM (Man-in-the-Middle attack): Devices attempt to pair at the exact moment [104]. Devices accidentally communicate after an attack has started [58]. During this period, the shared secret keys are not used for authentication. [58] Two devices are connected to the attacker after a successful assault, and they believe the pairing was effective [105,106].
Blue ants: An attacker uses flaws in out-of-date device firmware to listen in on phone conversations, send and get calls, establish connections to the World Wide Web, and do all of this outside approved users' awareness.
The blue snoring: Unauthorized use of the intended device is obtained by an intruder, who uses it to gather information and divert calls that come in. preparing for a strike With this method, the device's maker, approach, and software version will all be identified. Only when the BD ADDR of the intended gadget has been determined will the assault be successful[107].
Files Fuzzing attack: Fuzzing attacks occur when Bluetooth data packets are corrupted and sent to the target device's Bluetooth radio. An act of violence (BD ADDR). We begin our brute-force attack on the final three bits inside the BD ADDR while the initial three bits have been identified and unchangeable [108].
Worm attacks: An attacker uses a Trojan horse or malicious software to infect susceptible Bluetooth devices. Lasco worm, Cabir worm, and Scull's worm are all examples of these assaults.
Denial-of-service attacks target the protocol stack's physical layer or higher tiers. For example, Bluehost, Some of the more popular DoS assaults are BD ADDR replication, BlueSmack, Big NAK (Negative Acknowledgment), and L2CAP (Logical Link Control and Adaptation Layer Protocol) assured service[109].

***Near Field Communication(NFC)***

NFC is an international standardization organisation (ISO). NFC can only communicate within a few millimetres and has no security features. The most frequent attacks against NFC systems are listed below [110]. Eavesdropping. NFC transmissions may be intercepted or received by an attacker nearby, utilizing antennas that are more powerful and durable than those on mobile devices. Now a greater distance may be used to listen in on an NFC connection. Erasure of the data via an NFC interface; a hacker may change data. If the attacker updates the data in a way the victim is unaware of, DoS attacks may happen. Information restructuring during amplitude-modulated data transfer; an attacker could tamper with the original data. Messages containing hazardous and undesired content may be delivered when two devices exchange data the NFC (Data Exchange Format)NDEF Threats or the NFC Data Transmission Standard. Attackers would keep looking for composition attacks and use their weaknesses in weak signatures to gain trust[111].

## 4. Intrusion Detection System(IDS)

After connecting your devices, problems are likely to arise. Attacks may begin before, during, or even after linking the devices [112]. Man-in-the-middle assaults, for example, may benefit from the information attackers learned via pairing. [113] provides a thorough summary of Bluetooth security concerns. In the paragraphs below, we'll go through a handful of the most common Bluetooth assaults. When trying to figure out a personal identification number (PIN), an attacker will use this method when a device is paired or authorized. For example, using a frequency sniffer application, an attacker could get the Bluetooth Device Address (BD ADDR) and a random number of the target device (RAND). Then, following the discovery of the correct PIN combination, all other possibilities are examined using a brute-force method (similar to the E22 algorithm) [114].
A MAC spoofing effort: An attack occurs before encryption and while link keys are produced. Devices may verify one another's identities by exchanging created link keys. Then, hackers could be able to use other users' identities. They can halt communications and even change the data sent and received [115]. As they start to the couple, MIM attacks them. [116] After the assault, devices unwittingly communicate with one another [117,118]. Additionally,

it is prohibited to authenticate using shared secret keys during this period. Successful attacks link the two devices to the attacker and assume that the pairing was successful [119,120].

***Blue insects***

By exploiting security holes in outdated device firmware, an attacker may send and receive messages, listen in on phone conversations, and create connections to the Internet without the target's knowledge.

Snoring in public: The perpetrator obtains entry to the intended gadget and uses it to steal data and redirect incoming calls without the user's awareness. This approach may identify the device's firmware version, model, and manufacturer. It is impossible to carry out this attack When the objective's BD ADDR has been identified. When the Bluetooth wireless transmitter fails, that particular gadget will exhibit odd activity similar to a swarm of bees. Since the initial three bits of the BD ADDR are stable and popular, a brute-force analysis is employed to locate the final three bits[121].

Worm attacks: A hacker may employ a Trojan horse or other potentially harmful software to infect Bluetooth devices susceptible to this attack. Lasco worm, Cabir worm, and Scull's worm are all examples of these assaults. The protocol stack's physical layer or higher tiers often targets denial-of-service attacks. DoS attacks include battery depletion, BlueChip, BD ADDR replication, BlueSmack, Big NAK (Negative Acknowledgement), and L2CAP assured operation [122].

***Hybrid-Based Detection Techniques***

Many of the strategies discussed above are used in hybrid-based detection systems, which overcome the difficulty of detecting both old and new threats. For example, IP-connected IoT gadgets that use RPL for a method of routing throughout Inexpensively Wireless Private Area Networks. 6LoWPAN networks are proposed by [123] to use SVELTE, an IDS. A hybrid IDS was created to reconcile the processing and storage requirements of Anomaly-based and signature-based identification methods. It was anticipated that processing and storage costs would be equal for anomaly-based detection.

## 5. MachineLearning(ML)TechniquesforIDS

The IDS may be trained in specification-based detection without needing an ML approach. This section covers the various machine-learning techniques employed by IDSs in IoT scenarios.

***Naive Bayes(NB) Classifier***

Based on previous observations of similar events, this method forecasts the likelihood of an event occurring [124]. Machine learning might use NB classing to characterize normal and aberrant behaviour in supervised learning contexts. Regarding data categorization, NB stands out due to its ease of usage. NB computes the posterior probability and uses it in its labelling decision to classify traffic that is not labelled as normal or abnormal. It is possible to determine whether the communication is normal or abnormal by looking at the status flags, protocols, and latency of coming in and going out packets. Because NB classifiers are a quick and efficient approach to finding odd traffic, many IDSs utilize them. The training data has to be categorized, which may be done using binary or multiple labels. [125] The classification accuracy is decreased because the interdependencies between characteristics are not considered [126].

***K-nearest neighbour (KNN)***

KNN operates without requiring any parameters. The Euclidean distance(ED) calculates the spread between neighbours [127]. The KNN classification algorithm separates incoming data into various categories based on how closely the groups of previously observed data are to one another. Green squares for expected behaviour and red triangles for deviant behaviour are used to categorize instances. They may be used to determine how many of their neighbours fall into the same category as the unknown instance (blue hexagon). This unusual occurrence is categorized because it belongs to a well-established category. When putting an item into a class, the K closest neighbours are utilized. The categorization will change according to the assigned value of k. For k = 1, each red hexagon will be assigned to an unusual class; for k = 2 and k = 3, standard classes will be built. Research is required to identify the optimal value of k to assure the accuracy of this technique [128]. KNN-based categorization has been used in multiple investigations to identify User to Root (U2R) and Remote Local (R2L) dangers, abnormality and malware detection overall, and connected to the internet of detection of network attacks especially [129,130]. While basic, KNN needs to identify the ideal value of k and locate all vacant nodes.

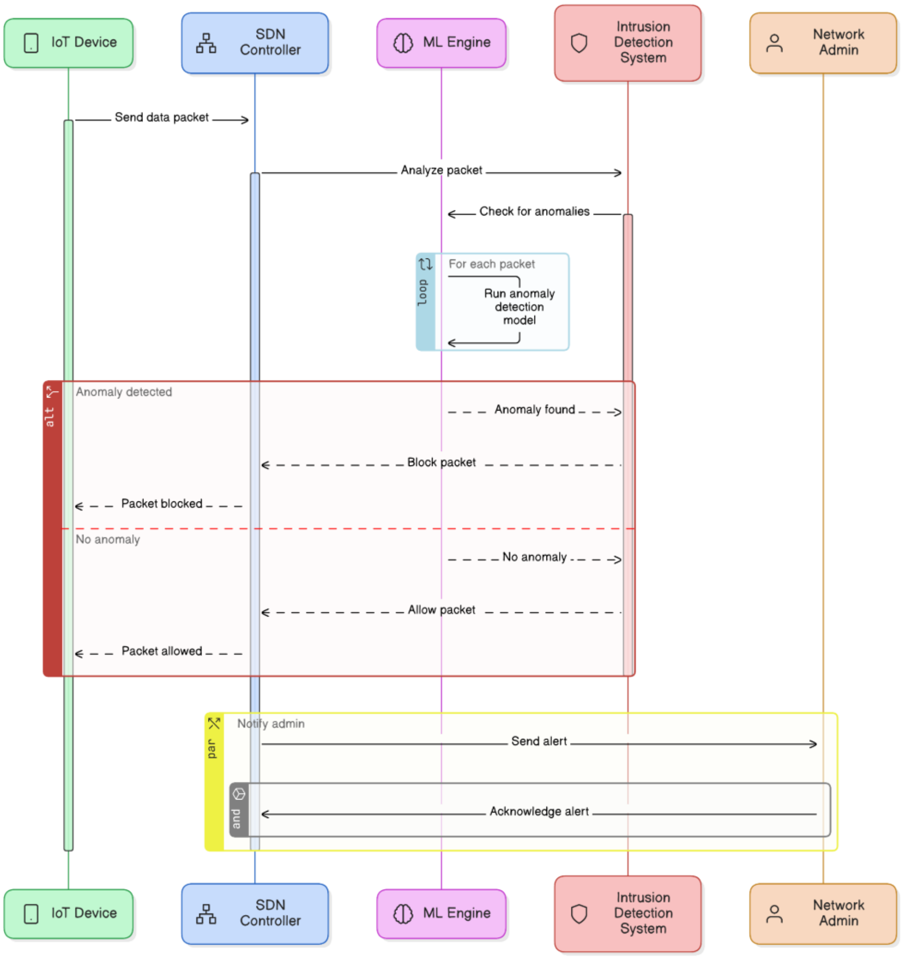

**Fig.2** Sequence Diagram of ML & DL based intrusion detection approch

***Decision Trees(DTs)***

To function, Decision Trees (DTs) need to first remove the distinctive characteristics of an information set and then construct a structured tree depending on the significance of every characteristic in the information being collected. Each property can be seen as a point in the structure of the tree, together with the data points that pertain to the branches to which it is linked. The origin of a tree is defined as a single node that perfectly divides it in half [131,132]. Applying the Gini scale and information acquisition [133], the most efficient starting point for splitting the initial data is identified. The model is built by DT algorithms, which classify it using two stages induction and deduction. To construct a DT, nodes and branches are initially inserted[134,135]. These nodes are initially empty, and a feature that distinguishes the training dataset samples is selected based on information gain and other variables[136]. The DT's origin vertex is then assigned to this feature. The selection of feature root nodes is ongoing as the training dataset's class overlap decreases. With more ease, the classifier can now distinguish between several instances of a particular class. The appropriate courses are assigned to each sub-leaf DT[137]. The inference step might begin after DT has been formed. By contrasting the newly formed DT with the previous DT, any occurrences of classes with unidentified features may be determined. The categorization of the new sample may now be complete with the acquisition of a matching leaf node, according to [138,139]. There are trade-offs regarding increased processing and storage complexity when using DTs as classifiers for intrusion detection [140,141]. [142] describes the research that uses DT to analyze network data to find malicious origins and identify DDoS assaults on the IoT.

***Support Vector Machines(SVMs)***

Two or more classes feature sets are used to build a hyperplane for the SVM classifier. SVMs can be helpful when there are numerous classes to be recognized but just a small data collection. They're great at spotting abnormalities in the data since they're based on statistical learning [128]. Because of their simplicity of use, SVMs can do online learning and Actual recognition of anomalies during intrusions. The research team of [134] used an altered version of SVM to identify anomalies in interactions between vehicles in Internet of Vehicles (IoV) networks. SVM is an outstanding storage and RAM solution. SVM-based IDSs produced more precise findings in a connected device than various other machine learning methods (e.g., DTs, NB, Random Forest). When information can't be linearly separated into different columns, an optimal kernel function is utilised. It is now impossible to use this approach at the requisite classification level [143, 144].

***Ensemble Learning(EL)***

Before making a classification decision that is accepted by the majority, classifiers should use their specialized expertise. Integrating the outputs of multiple homogeneous/heterogeneous learners improves the effectiveness of classification [145,146]. The research investigation that laid the groundwork for EL discovered that application-specific and relevant information influences how precise any ML categorization approach is[147]. There cannot be a "one size suits all' artificial intelligence method, therefore EL-like combinations may be excellent for generalised purposes to enhance reliability by minimising variability and avoiding excessive fitting [148].. However, the accuracy of EL decreases as temporal complexity rises when many classifiers are applied concurrently [149,150]. Numerous research has examined the applicability of EL for intrusion detection[151,152]. A lightweight EL framework with broad applicability for online outlier detection in IoT networks has been established after research on the viability of EL in environments with limited resources, such as IoT[153]. According to this study, an EL algorithm gave more accurate findings than each member classifier [154].

***Random Forest(RF)***

The discipline of supervised machine learning includes RFs. Combining several DT leads in an RF predicts classification outcomes that are more accurate and error-free [155,156]. Instructing DTs to give categorization findings based on the majority vote results is a standard procedure [157]. Two distinct classification techniques, one using all member DTs and the other only using the training set of DTs, may be employed to generate the rule-subset for both RF. Findings are more reliable and accurate when there are no feature selections and fewer inputs [158]. RF has been shown in several studies [159,160] to be an effective method for finding intrusions and anomalies in connected devices. Based on subsequent studies [161][162], RF beat KNN, ANN, and SVM in identifying DDoS in IoT networks since it needed less parameters for input and might prevent the costly calculations involved in choosing features in actual time IDS."***k-Means Clustering***

This unsupervised strategy relies on the discovery of k clusters across data sets. A collection is formed for each piece of data we gather. The distribution of samples among the k clusters is used to compute the Euclidean distance(ED), which is the square of the distribution. No further cluster alterations can be made at this point in the operation. For the k-means clustering approach to work, the k number must be chosen carefully, and the sample dataset must be uniformly distributed throughout the k groups. K-means clustering was found acceptable for anomaly detection by examining feature similarity in a prior study [162,163]. To improve performance, the authors proposed DT and k-means clustering [164] for IoT network anomaly detection.

***Principle Component Analysis(PCA)***

A method for identifying anomalies, PCA cannot be used to select or minimize features from massive datasets. However, additional machine learning classifiers may be used to identify abnormalities in an IoT network. By applying PCA, you may reduce a vast number of variables to a smaller set of features while keeping all of the pertinent information that was previously acquired[165,166]. Classifiers like PCA have been used in research to find IoT network abnormalities**.**

### 5.1 Deep Learning(DL) Techniques for IDSs

Large dataset scenarios are ones where DL algorithms outperform ML approaches. Since IoT settings are known for creating enormous numbers and a broad diversity of data, DL is necessary for IoT security applications. DL can also automatically model complex feature sets based on the test data [167,168]. Deep linking in IoT networks is another advantage of DL algorithms claims [169]. Therefore, IoT-based devices may interact automatically and carry out preset cooperative actions without the need for human intervention. Deep learning (DL) methods may be categorized as a subset of machine learning (ML) techniques that use many non-linear stages of processing to extract feature sets due to their capacity to produce hierarchical representations from complicated deep structures[170]. These feature sets must first undergo appropriate abstraction and pattern recognition adjustments. This part will go through the most widely used DL-based methods for building an IDS. The DL approach is explained in the following subsections[171].

***Recurrent Neural Networks(RNNs)***

When data is handled consecutively, RNN operates successfully. Unlike previous neural networks, this one, 's Instead of forwarding propagation, the output depended on back propagation. To analyze data sequentially and discover previously undetected multi-dimensional changes in recurrent component units, an RNN contains a temporal layer[172,173]. The current state of the neural network is represented by the ongoing updating of these hidden units in response to the input they receive. An RNN approach implies that a future concealed state would trigger an initial unrevealed state to evaluate the present undisclosed neural network state. In instances involving the Internet of Things (IoT) where there is a large amount of sequential information, like internet traffic circulates, Recurrent Neural Networks (RNNs) are essential for detecting system breaches[174,175]. Prior studies have investigated using Recurrent Neural Networks (RNNs) to analyse network traffic and detect time-series-based risks such as network intrusions [176]. A new investigation introduces an Intrusion Detection System (IDS) that utilises a complex structure consisting of deep complex Recurrent Neural Networks (RNNs) and a transmitter processing structure. The next stage of recurrent neural network (RNN) training involves acquiring the ability to identify common Internet of Things (IoT) threats such as R2L, Dos, or U2R. IDS was constructed using network designs with LSTM layouts, depending on recurrent neural networks (RNN). LSTM-based RNNs possess the fundamental attribute of retaining data or cell states for future utilisation. Because of these characteristics, they were well-suited for the evaluation of thing information[177]. LSTM networks are recommended for identifying anomalies in sequences of sequential data. Scientists have utilised LSTM-based RNNs alongside various types of RNNs to identify abnormalities and unauthorised access in IoT networks [178-183]. Although RNN-based time-series information prediction has shown encouraging outcomes, it remains difficult to detect abnormal traffic utilising these forecasts.

### *Convolutional Neural Network(CNN)*

When data processing has to be done sequentially, RNN, a discriminative DL approach, works well. In contrast to conventional neural networks, it employs back-propagation rather than forward propagation for output. To analyze data sequentially and find previously undetectable changes in recurrent component units on multiple dimensions, RNNs include a temporal layer [184]. Every fresh time input is received, the neural network's hidden units are modified, resulting in the outer representation of the current state. An RNN algorithm anticipates that later states will trigger earlier conditions that haven't yet been revealed to analyze the neural network's current hidden state. Through their outputs, the neurons in the layer above provide feedback to the neurons in this state.

Recurrent Neural Networks (RNNs) play a crucial role in ensuring the safety of Internet of Things (IoT) programmes, particularly in attack identification. This is due to the vast quantities of sequential information that are produced in the context of IoT. Previous research [185] has demonstrated that an RNN is highly proficient in identifying vulnerabilities in networks by analysing the behaviour of network traffic. One proposed solution is to use an Intrusion Detection System (IDS) that incorporates Recurrent Neural Networks (RNNs) for each filter and level of cascading filtration [186]. Subsequently, Recurrent Neural Networks (RNNs) undergo training to identify prevalent Internet of Things (IoT) vulnerabilities such as R2L, Dos, U2R, and Probe.

RNN-based LSTM network structures, which are a specific type of recurrent neural network, were also employed in the creation of Intrusion Detection Systems (IDS). An essential characteristic of LSTM-based RNNs is their ability to retain and utilise data or cell state for future use within the network. These properties make them well-suited for processing time-varying data. The most effective approach for detecting anomalies in time-lapse order data is to employ LSTM networks. In a study conducted in 187, researchers utilised LSTM-based RNNs and other types of RNNs to detect anomalies and attacks in connected devices. Recurrent Neural Networks (RNNs) have effectively forecasted time series data. Nonetheless, it remains difficult to detect atypical traffic based on their forecasts.

### *Deep Auto Encoders(DAEs)*

An unsupervised technique uses a decoder and a hidden layer to repeat input at the output while preserving the details of the input representation code [188,189]. An AE neural network's encoder function converts the gathered information into a language the network can comprehend. Reconstruction mistakes must be kept to a minimum during training [190,191]. Now, AE may be used to take features out of datasets. They have the drawback of requiring a substantial amount of computer resources. Research has demonstrated that DAEs are superior compared to SVM and KNN in accurately identifying network-based viruses [192]. Kitsune [41] created an internet-based, efficient Intrusion Detection System (IDS) for Internet of Things (IoT) situations. The system utilises anomaly recognition and autonomous learning techniques, employing multiple deep auto-encoders. The researchers present compelling evidence demonstrating the superior accuracy of their approach compared to current machine learning (ML) and deep learning (DL) approaches.

### *Restricted Boltzmann Machine(RBM)*

Unsupervised learning constructs a complex, creative, and non-directed network. There are no connections between cells on any level of an RBM. A Restricted Boltzmann Machine (RBM) consists of two types of levels: visible ones and unseen layers. The viewable layer comprises the previously identified input parameters, whereas the invisible layer, which is consisting of multiple layers, encompasses the unidentified parameters that are entered. When a dataset is organised in a hierarchical manner, the latent variables are moved to the subsequent layer. Several studies utilised an RBM-based device for network/IoT security detection [193,194]. Nevertheless, the Restricted Boltzmann Machine (RBM) requires significant computational resources, which poses a challenge when attempting to implement it on low-power Internet of Things (IoT) devices. Moreover, a solitary Restricted Boltzmann Machine (RBM) is incapable of representing additional properties. A Deep Belief Network can utilise many Restricted Boltzmann Machine (RBM) layers to address this limitation.

***Deep Belief Network(DBN)***

DBNs, generative algorithms based on unsupervised learning, were created by stacking two or more RBMs[195]. After unsupervised training, each layer functions very well. As each layer regains its essential qualities before exercise, A softmax level is provided at the highest level for modification, as described in reference [196]. Nevertheless, there is limited empirical support to demonstrate the effectiveness of Dynamic Bayesian Networks (DBNs) in an Internet of Things (IoT) context, despite previous research suggesting that DBNs outperform ML methods in detecting harmful attacks[197].

***Generative Adversarial Network(GAN)***

A combination of deep learning strategy concurrently produces both productive and discriminatory algorithms [198]. The discriminatory algorithm utilises the statistical characteristics of the information set and selections to make predictions about the authenticity of a certain instance from an initial dataset [199]. Discrimination, on the other hand, tries to distinguish between actual training data and fictitious data created by the generative model. The binary classification D(x) in this situation reveals whether or not the output is authentic (generated). Unfortunately, both models have a terrible correlation between correct/incorrect classification and accuracy and performance. Thus, during each cycle, models are often modified. A study was conducted to assess the efficacy of the GAN approach in identifying abnormal activity in WoT environments. As a result, the GAN method can generate samples that mimic zero-day threats to understand different attack situations. Nevertheless, the utilisation of GAN poses difficulties due to its rigorous training requirements and unpredictable results.

***Ensemble of DL Networks(EDLN)***

According to the claim above, a classifier composed of many machine learning classifiers seems more accurate. Like multiple DL algorithms, several ML algorithms may be employed in an ensemble to provide superior results. DL algorithms may be generative, discriminative, or hybrid in EDLNs. EDLNs can now better handle complicated problems in settings with various characteristics and uncertainties. A homogeneous EDLN, in contrast to a heterogeneous one, only contains classifiers from a single genre. Both compositions are intended to boost output and provide precise outcomes. Further study is needed to determine if EDLN can increase the security system's efficacy and accuracy [200].

### 5.2 Datasets Available for IoT Security

For any IDS analysis, a current, trustworthy dataset that includes both typical and abnormal behaviour must be employed. Early IDS research depended heavily on the KDD99 dataset since few alternatives were available then. However, A study was conducted to assess the efficacy of the GAN approach in identifying abnormal activity in WoT environments. As a result, the GAN method can generate samples that mimic zero-day threats to understand different attack situations. Nevertheless, the utilisation of GAN poses difficulties due to its rigorous training requirements and unpredictable results.

KDD99: Researchers at the Lincoln Laboratory at MIT explored how intrusion detection systems might distinguish between an attack and a standard connection as part of the DARPA98 project. The KDD CUP 99 dataset underwent filtration for the World Knowledge Acquisition and Information Mining Techniques Challenge [208]. The majority of scholars have widely utilised the dataset for most of the past two decades. Due of its exclusive accessibility, this dataset has been extensively utilised in studies to evaluate the precision of the classification. Nevertheless, the limitations of KDD-99, including its outdated nature, prejudiced objectives, lack of consistency among the data used for training and testing data sets, trend repetition, and unimportant characteristics, render it unsuitable for current situations[203].

National Security Agency KDD: NSL-KDD was created by the researchers whose findings were reported in [204] to solve KDD-99's inadequacies. The cases targeted by this KDD-99 resampling are those that classifiers trained on the original KDD-99 are most likely to overlook. The producers of the dataset agree that there are still problems with the data, such as an under-representation of assaults with a small footprint. The name of the database is DEFCON. The DEFCON-8 dataset, established in 2000, comprises possible threats to security like port inspection and buffer explosion. In 2002, a revised edition of the DEFCON-10 database was released. This version includes FTP-over-telnet messages with errors, operator authority, port checks, and comprehensive assaults. Unlike practical internet traffic, traffic generated in capture-the-flag (CTF) competitions mostly comprises assault information rather than underlying traffic. As a result, it is less suitable for evaluating intrusion detection systems (IDS). The information set is commonly employed for assessing alert connection algorithms.

The Centre for Applied Internet Data Analysis (CAIDA) provides datasets spanning between 2002 to 2016.

CAIDA has made accessible three files containing information relating to a distributed denial of service (DDoS) assault that occurred in August 2007. These datasets are the CAIDA DDoS, which consists of various kinds of information noticed on an OC48 hyperlink, and the CAIDA web traces 2016, which consist of passively transmitted traces collected by the Equinix-Chicago track on the fast Internet foundation [207]. Information on the protocol, payload, and destination may be found in these anonymous databases, which are created for a specific incident or attack type. However, the lack of detailed information on attack occurrence makes these benchmarking datasets worthless, as discussed in[205].

LBNL(Lawrence Berkeley National Laboratory ): The LBNL dataset contains anonymised traffic statistics, namely header characteristics. The information set at the Lawrence Berkeley National Laboratory was generated utilising real inbound bubbly, and route traffic information collected by two edge routers [206]. As a result, no established categorization system was developed, and no new features [206.207].

UNSW: The researchers of [208] at UNSW Canberra created the UNSW-NB15 dataset to evaluate IDS. The IXIA PerfectStorm application was used by researchers from the Australian Center for Cyber Security (ACCS) to produce a mix of malicious and benign traffic over two days, in sessions lasting 16 and 15 hours. They created a dataset of 100 GB with a sizable number of brand-new files representing features. The NB15 dataset will take the place of the KDD99 dataset that was previously disclosed. Its ten targets are backdoors, shell code, generic, reconnaissance, fuzzes, worms, DoS, and analysis [208]. In addition, nine weird targets and one honourable target are also present. The dataset was created in a synthetic setting that mimicked assault strategies.

The ISCX(Installation Support Center of Expertise) datasets [209]: The Canadian Institute for Cybersecurity uses many datasets created by independent researchers, academic institutions, and the corporate sector worldwide. The IPS/IDS dataset on AWS (CSE-CIC-IDS2018), the IPS/IDS dataset on CICIDS2017, the CIC DoS dataset (application-layer), the ISCX Botnet dataset, the ISCX IDS 2012 dataset, the ISCX Android Botnet dataset, and the ISCX NSL-KDD dataset are a few datasets that appear to be pertinent to our investigation. CICIDS2017, the most recent dataset, is relevant to our research. This dataset, identical to actual data [209], comprises the most recent relatively common assaults. The CICIDS2017 uses the B-Profile technology to provide precise user-related background traffic for its many attack scenarios. Based on the FTP(File Transfer Protocol), SSH(Secure Shell), HTTP(Hypertext Transfer Protocol), HTTPS(Hypertext Transfer Protocol Secure), and email protocols, they built the abstract behaviour of 25 individuals for this dataset. However, the datasets' lack of ground truth made the labelling process less accurate. In addition, the intricacy of entire networks may make it difficult to use the profiling idea employed to create these datasets[209].

BoT-IoT (210) At the UNSW Canberra Cyber Center's Cyber Range Lab, a realistic network environment was used to build the BoT-IoT dataset. The ecosystem contains both genuine traffic and botnet traffic. Researchers propose a testbed environment to address the current dataset's deficiencies in acquiring precise labelling, the most recent and successful attack type, and extensive network information. The BoT-IoT dataset was compared to the other datasets mentioned above to determine how reliable it is about them. Various file types, including CSV(comma-separated values) files, freshly created argus files, and the original Packet Capture Application Programming (PCAP) files, are accessible as the dataset's source files. The data were divided depending on the kind and subtype of assaults to facilitate labelling. The collection includes OS and service scanning, keylogging, DoS, and DDoS attacks. The data set for BoT-IoT [210] categorises DDoS and DoS assaults further into categories. Due to the deployment of the honeypots, manual labelling and anonymization were not feasible for this dataset. Since there weren't many attacks on the honeypots that could be found, it had a limited comprehension of the network traffic. BoT-IoT, according to the authors, analyses Telnet-based attacks on a range of IoT devices with a range of CPU(Central Processing Unit) architectures, including MIPS(Million Instruction Per Second.), ARM9 (Advanced RISC Machines), and PPC(pay-per-click). During the 39 days of operation, 76,605 attempts to download malware binaries were performed from 16,934 different IP addresses. Since honeypots that handle the Telnet protocol, such as telnet password honeypot and honey, cannot control the massive amount of incoming instructions sent by the attackers, the authors contend that none of these programs could have been discovered. The most current dataset was produced due to the authors' research on online network IDS, which focuses mainly on the assessment of IDS for IoT networks[211].

The investigators employed two separate networks for their experiment. One network consisted of IP cameras that were used for video surveillance, while the additional network consisted of three PCs & nine connected devices. Each of the connected devices in the second network was intentionally infested with the botnet known as Mirai virus. The scientists conducted six different types of attacks, all of which posed a threat to the confidentiality and availability of the footage uplinks. The authors extensively elaborate on the assaults and the system topologies in their written works. Furthermore, the researchers generated a collection of vectors of features for every one of the nine seasons, from that they later gathered information. Some of the assault's methodologies are OS Scan, Fuzzing, Video Injection, ARP, MiTM, Active Wiretap (Simple Service Discovery Protocol), SSDP Flood, SYN DoS (Secure Socket Layer), SSL Negotiations, and Mirai[212].

## 6. Conclusions

IoT technologies have gained popularity in diverse scenarios during the past decade due to their capacity to convert tangible objects from different application domains into Web hosts. Nevertheless, users' security and privacy are jeopardised due toof consumers are jeopardised as a result of security vulnerabilities in IoT. Therefore, security measures for the Internet of Things must be more reliable. Machine and deep learning-based Intrusion Detection Systems (IDS) are crucial ways for ensuring security in the Internet of Things (IoT). This paper provides a concise overview of the machine learning (ML) and deep learning (DL) techniques used for detecting unauthorised access in Internet of Things (IoT) networks and gadgets, namely in intrusion detection systems (IDS). The topics of SDN design, protocols, weaknesses in systems, and protocol-level assaults have garnered significant interest. Next, there is a section that evaluates the research presented in the existing body of literature. Additionally, a compilation of several datasets suitable for investigating the safety of IoT devices is included. This study uses machine learning (ML) and deep learning (DL) algorithms for intrusion detection in IoT gadgets and networks. Its objective is to give academics a comprehensive understanding of the various security challenges that exist in the IoT domain and offer feasible solutions.

## REFERENCES

[1] A Ray, S.; Jin, Y.; Raychowdhury, A.The changing computing paradigm with the internet of things: A tutorial introduction.IEEEDes.Test2016,33,76–96.

[2] Diechmann, J.; Heineke, K.; Reinbacher, T.; Wee, D.The Internet of Things: How to Capture the Value of IoT.Technical Report, Technical Report May. 2018, pp. 1–124. Available online: https://www.mckinsey.com/featured-insights/internet-of-things/our-insights/the-internet-of-things-how-to-capture-the-value-of-iot# (accessed on July 2020).

[3] Khan, R.; Khan, S.U.; Zaheer, R.; Khan, S.Futureinternet: The internet of things architecture, possible applications, and key challenges. In Proceedings of the 2012 10th International Conference on Frontiers of Information Technology, Islamabad, India,17–19 December 2012; pp. 257–260.

[4] Yang, Z., Peng, Y., Yue, Y., Wang, X., Yang, Y., & Liu, W. (2011). Study and application of the architecture and key technologies for IoT. 2011 International Conference on Multimedia Technology, 747-751.

[5] Atzori,L.;Iera,A.;Morabito,G.Theinternetofthings: Asurvey.Comput.Netw.2010,54,2787–2805.

[6] Torkaman,A.;Seyyedi,M.AnalyzingIoTreferencearchitecturemodels.Int.J.Comput.Sci.Softw.Eng.2016,5,154.

[7] Chaqfeh, M.A.; Mohamed, N. Challenges in middleware solutions for the internet of things. In Proceedingsofthe2012InternationalConferenceonCollaborationTechnologiesAndSystems(CTS),Denver,CO,USA,21–25May2012;pp.21–26.

[8] Moustafa, N.; Creech, G.; Sitnikova, E.; Keshk, M.Collaborative anomaly detection framework for handling big data of cloud computing.In Proceedings of the2017 Military Communications and Information SystemsConference(MilCIS),Canberra,ACT,Australia,14–16November2017;pp.1–6.

[9] Moustafa, N.; Choo, K.K.R.; Radwan, I.; Camtepe, S.OutlierDirichlet mixture mechanism: Adversarialstatisticallearningforanomalydetectioninthefog.IEEETrans.Inf.ForensicsSecur.2019,14,1975–1987.

[10] Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead.Comput.Netw.2015,76,146–164.

[11] Kolias,C.;Kambourakis,G.;Stavrou,A.;Voas,J.DDoSintheIoT:Miraiandotherbotnets.Computer2017,50,80–84.

[12] Al-garadi, M.A., Mohamed, A.M., Al-Ali, A.K., Du, X., Ali, I., & Guizani, M. (2020). A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. IEEE Communications Surveys & Tutorials, 22, 1646-1685.

[13] Kolias, C.; Stavrou, A.; Voas, J.; Bojanova, I.; Kuhn, R.Learning internet-of-things security hands-on'.IEEESecur.Priv.2016,14,37–46.

[14] Marsden, T.; Moustafa, N.; Sitnikova, E.; Creech, G. Probability risk identification based intrusion detection system for SCADA systems. In International Conference on Mobile Networks and Management; Springer: Berlin, Germany,2017; pp. 353–363.

[15] Moustafa, N.; Misra, G.; Slay, J.Generalized outlier gaussian mixture technique based on automated association features for simulating and detecting web application attacks. IEEE Trans. Sustain. Comput. 2018,doi:10.1109/TSUSC.2018.2808430.

[16] Modi, C.; Patel, D.; Borisaniya, B.; Patel, H.; Patel, A.; Rajarajan, M.A survey of intrusion detection techniques inc loud.J.Netw.Comput.Appl.2013,36,42–57.

[17] Rizwan, R.; Khan, F.A.; Abbas, H.; Chaudhary, S.H. Anomaly detection in wireless sensor networks using the immune-based bio-inspired mechanism. Int. J. Distrib.Sens.Netw.2015,11,684952.

[18] Moustafa, N.; Creech, G.; Slay, J.Anomaly detection system using beta mixture models and outlier detection. In Progress in Computing, Analytics and Networking; Springer: Berlin, Germany,2018; pp. 125–135.

[19] Alrajeh, N. A., Khan, S.,&Shams, B. (2013). Intrusion Detection Systems in Wireless Sensor Networks: A Review. International Journal of Distributed Sensor Networks. https://doi.org/10.1155/2013/167575

[20] Mitchell, R.; Chen, I. R. A survey of intrusion detection techniques for cyber-physical systems.ACM Comput.Surv.(CSUR)2014,46,55.

[21] Mishra, Awadhesh & Nadkarni, Ketan & Patcha, Animesh. (2004). Intrusion Detection in Wireless Ad Hoc Networks. Wireless Communications, IEEE. 11. 48 - 60. 10.1109/MWC.2004.1269717.

[22] Anantvalee, T.; Wu, J.A survey on intrusion detection in mobile ad-hoc networks. In Wireless Network Security; Springer: Berlin, Germany, 2007; pp. 159–180.

[23] Kumar, S.; Dutta, K. Intrusion detection in mobile ad-hoc networks: Techniques, systems, and future challenges. Secure. Commun. Netw. 2016,9, 2484–2556.

[24] Sfar,A.R.; Natalizio,E.;Challah,Y.; Chtourou, Z.A road map for security challenges in the Internet of Things. Digit. Commun. Netw.2018,4,118–137.

[25] Keshk, M.; Moustafa, N.; Sitnikova, E.; Creech, G. Privacy preservation intrusion detection technique for SCADA systems. In Proceedings of the 2017 Military Communications and Information Systems Conference(MilCIS), Canberra, ACT, Australia,14–16 November 2017; pp.1–6.

[26] Zhao, K.; Ge, L. A survey on the internet of things security. In Proceedings of the 2013 Ninth International Conference on Computational Intelligence and Security, Leshan, China,14–15 December 2013; pp. 663–667.

[27] Kumar, J.S.; Patel, D.R.A survey on internet of things: Security and privacy issues. Int. J. Comput. Appl. 2014, 90, doi:10.5120/15764-4454.

[28] Suo, H.; Wan, J.; Zou, C.; Liu, J.Security in the internet of things: A review. In Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, China, 23–25 March 2012; Volume 3, pp. 648–651.

[29] Kosice, D. E.; Bouabdallah, A.; Lakhlef, H. Internet of things security: A top-down survey. Comput. Netw. 2018, 141, 199–221.

[30] Benkhelifa, E.; Welsh, T.; Hamouda ,W. A critical review of practices and challenges in intrusion detection systems for IoT: Toward universal and resilient systems. IEEE Commun. Surv. Tutor. 2018, 20, 3496–3509.

[31] Abduvaliyev, A.; Pathan, A.S.K.; Zhou, J.; Roman, R.; Wong, W.C.On the vital areas of intrusion detection systems in wireless sensor networks.IEEE Commun.Surv.Tutor.2013,15,1223–1237.

[32] Granja, J.; Monteiro, E.; Silva, J.S.Security for the internet of things: A survey of existing protocols and open research issues.IEEE Commun.Surv.Tutor.2015,17,1294–1312.

[33] Zarpelao, B. B.; Miani, R. S.; Kawakami, C. T.; de Alvarenga, S. C. A survey of intrusion detection in Internet of Things. J. Netw. Comput. Appl. 2017, 84, 25–37.

[34] Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT Security Techniques Based on Machine Learning. ArXiv, abs/1801.06275.

[35] Buczak, A.L.; Guven, E.A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Commun. Surv. Tutor. 2015, 18, 1153–1176.

[36] Mishra, P.; Varadharajan, V.; Tupakula, U.; Pilli, E. S. A detailed investigation and analysis of machine learning techniques for intrusion detection. IEEE Commun.Surv.Tutor.2018,21,686–728.

[37] Chaabouni, N.; Mosbah, M.; Zimmer, A.; Sauvignac, C.; Faruki, P. Network Intrusion Detection for IoT Security based on Learning Techniques.IEEE Commun.Surv.Tutor.2019,21,2671–2701.

[38] Lawal, M. A.; Shaikh, R. A.; Hassan, S. R. Security analysis of network anomalies mitigation schemes in IoT networks. IEEE Access 2020, 8, 43355–43374.

[39] Garg, S.; Kaur, K.; Batra, S.; Kaddoum, G.; Kumar, N.; Boukerche, A. A multi-stage anomaly detection scheme for augmenting the security in IoT-enabled applications. Future Gen. Comput. Syst. 2020, 104, 105–118.

[40] Garg, S.; Kaur, K.; Kumar, N.; Kaddoum, G.; Zomaya, A.Y.; Ranjan, R.A hybrid deep learning-based model for anomaly detection in cloud data center networks.IEEE Trans. Netw. Serv. Manag. 2019, 16, 924–935.

[41] Mirsky, Y.; Doitshman, T.; Elovici, Y.; Shabtai, A. Kitsune: An ensemble of autoencoders for online network intrusion detection. arXiv 2018, arXiv: 1802.09089.

[42] Sethi, P.; Sarangi, S. R. Internet of things: Architectures, protocols, and applications. J. Electr. Comput. Eng.2017, 2017, doi:10.1155/2017/9324035.

[43] Wu, M.; Lu, T. J.; Ling, F. Y.; Sun, J.; Du, H. Y. Research on the architecture of the internet of things In Proceedings of the 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICE), Chengdu, China,20–22 August 2010; Volume5.

[44] Tan, L.; Wang, N. Future internet: The internet of things. In Proceedings of the 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICE), Chengdu, China, 20–22 August 2010; Volume5.

[45] ITU, T.Telecommunication Standardization Sector of ITU. Annexe CRTP Payload Format H1993, 261, 108–113.

[46] Weyrich, M.; Ebert, C. Reference architectures for the internet of things. IEEE Soft w. 2015, 33, 112–116.

[47] Fremantle, P.A Reference Architecture for the Internet of Things.WSO2 White Paper. 2015. Available online: https://docs.huihoo.com/wso2/wso2-whitepaper-a-reference-architecture-for-the-internet-of-things. pdf(accessedon13July2020).

[48] Green, J. The Internet of Things Reference Model; Internet of Things World Forum: Geneva, Switzerland, 2014; pp. 1–12.

[49] Note, S.; Siddiqi, M.; Gharakheili, H.H.; Sivaraman, V.; Borelli, R. An experimental study of security and privacy risks with emerging household appliances. In Proceedings of the2014 IEEE Conference on Communications and Network Security, SanFrancisco, CA, USA, 29–31 October 2014; pp. 79–84.

[50] Banerjee, A.; Venkata Subramanian, K. K.; Mukherjee, T.; Gupta, S. K. S. Ensuring safety, security, and sustainability of mission-critical cyber-physical systems. Proc. IEEE 2011, 100, 283–299.

[51] Law, R.; Youssef, A.M. Security tradeoffs in cyber-physical systems: A case study survey on implantable medical devices. IEEE Access 2016, 4, 959–979.

[52] Wamba, S. F.; Anand, A.; Carter, L. A literature review of RFID-enabled healthcare applications and issues. Int. J. Inf. Manag. 2013, 33, 875–891.

[53] Malaria, K.; Wang, L. Securing wireless implantable devices for healthcare: Ideas and challenges. IEEE Commun. Mag. 2009, 47, 74–80.

[54] Keshk, M.; Sitnikova, E.; Moustafa, N.; Hu, J.; Khalil, I. An Integrated Framework for Privacy-Preserving based Anomaly Detection for Cyber-Physical Systems. IEEE Trans. Sustain. Comput. 2019, doi: 10.1109/TSUSC.2019.2906657.

[55] Bertino, E.; Islam, N. Botnets and internet of things security. Computer 2017, 50, 76–79.

[56] Nesterenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scaleIoTexploitations. IEEE Commun. Surv. Tutor. 2019, 21, 2702–2733.

[57] Faruki, P.; Bharmal, A.; Laxmi, V.; Ganmoor, V.; Gaur, M.S.; Conti, M.; Rajarajan, M. Android security: A survey of issues, malware penetration, and defenses. IEEE Commun. Surv. Tutor. 2014, 17,998–1022.

[58] Huang, J.; Zhang, X.; Tan, L.; Wang, P.; Liang, B. Android: Detecting steal thy behaviors in android applications by the user interface and program behavior contradiction. In Proceedings of the 36th International Conference on Software Engineering, Hyderabad, India, 31 May–7 June 2014; pp. 1036–1046.

[59] Alaba, F.A.; Othman, M.; Hashem, I. A. T.; Alotaibi, F. Internet of Things security: A survey. J. Netw. Comput. Appl. 2017, 88, 10–28.

[60] Bakara, C. Security issues and challenges for the IoT-based smart grid. Procedia Comput. Sci.2014, 34, 532–537.

[61] Steinhubl, S. R.; Muse, E. D.; Topol, E. J. The emerging field of mobile health. Sci. Transl. Med. 2015, 7, 283rv3.

[62] Stergiou, C.; Psannis, K.E.; Kim, B.G.; Gupta, B.Secure integration of IoT and cloud computing. Future Gen. Comput. Syst. 2018, 78, 964–975.

[63] Lee, K.; Murray, D.; Hughes, D.; Joosen, W. Extending sensor networks into the cloud using amazon web services. In Proceedings of the 2010 IEEE International Conference on Network Embedded Systems for Enterprise Applications, Suzhou, China,25–26 November 2010; pp. 1–7.

[64] Botta, A.; De Donato, W.; Persico, V.; Pescapé, A. Integration of cloud computing and internet of things: A survey.Future Gen. Comput. Syst. 2016, 56, 684–700.

[65] Bhattasali, T.; Chaki, R.; Chaki, N. Secure and trusted cloud of things. In Proceedings of the 2013 Annual IEEE India Conference(INDICON), Mumbai, India, 13–15 December 2013; pp.1–6.

[66] Subashini, S.; Kavitha, V.A survey on security issues in service delivery models of cloud computing. J. Netw. Comput. Appl. 2011, 34, 1–11.

[67] Zhou, W.; Jia, Y.; Peng, A.; Zhang, Y.; Liu, P. The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges set to be solved. IEEE Internet Things J. 2018, 6, 1606–1616.

[68] Ronen, E.; Shamir, A.; Weingarten, A.O.; O'Flynn, C. IoT goes nuclear: Creating a ZigBee chain reaction. In Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2017; pp. 195–212.

[69] Jing, Q.; Vasilakos, A.V.; Wan, J.; Lu,J.; Qiu, D. Security of the Internet of Things: Perspectives and challenges.Wirel. Netw. 2014, 20, 2481–2501.

[70] Karlof, C.; Sastry, N.; Wagner, D. Tiny Sec: A link layer security architecture for wireless sensor networks. In Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, Baltimore, MD, USA, 3–5 November 2004; pp. 162–175.

[71] Garg, S.; Kaur, K.; Kaddoum, G.; Ahmed, S.H.; Jayakody, D.N.K. SDN-based secure and privacy-preserving scheme for vehicular networks: A5 G perspective. IEEE Trans. Veh. Technol. 2019, 68, 8421–8434.

[72] Perera, C.; Zaslavsky, A.; Christen, P.; Georgakopoulos, D. Context aware computing for the internet of things: A survey. IEEE Commun. Surv. Tutor. 2013, 16, 414–454.

[73] Akyildiz, I.F.; Su, W.; Sankara Subramaniam, Y.; Cayirci, E. A survey on sensor networks.IEEE Commun. Mag. 2002, 40, 102–114.

[74] Abdul-Ghani, H. A.; Konstantas, D.; Mahyoub, M.A comprehensive IoT attack survey based on the abuilding-blocked reference model. Int. J. Adv. Comput. Sci. Appl. 2018, 9, 355–373.

[75] Khattab,A.;Jeddi,Z.;Amini,E.;Bayoumi,M.RFIDSecurity:ALightweightParadigm;Springer:Berlin,Germany,2016.

[76] Fan, X.; Susan, F.; Long, W.; Li, S.Security Analysis of Zigbee. 2017. Available online: https://courses.csail.mit.edu/6.857/2017/project/17.pdf(accessedon13July2020).

[77] Lee, K.; Lee, J.; Zhang, B.; Kim, J.; Shin, Y.An enhanced Trust Center based authentication in ZigBee networks.In International Conference on Information Security and Assurance; Springer: Berlin, Germany, 2009; pp.471–484.

[78] Dini, G.; Tiloca, M. Considerations on security in ZigBee networks. In Proceedings of the the2010 IEEEInternational Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, Newport Beach, CA, USA,7–9 June 2010; pp. 58–65.

[79] Vidgren, N.; Haataja, K.; Patino-Andres, J. L.; Ramirez-Sanchis, J.J.; Toivanen, P. Security threats in ZigBee-enabled systems: Vulnerability evaluation, practical experiments, countermeasures, and lessons learned. In Proceedings of the 2013 46th Hawaii International Conference on System Sciences, Maui, HI, USA,7–10 January 2013; pp. 5132–5138.

[80] Kolias, C.; Kambourakis, G.; Stavrou, A.; Gritzalis, S.Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset.IEEE Commun.Surv. Tutor.2015,18,184–208.

[81] IEEE Computer Society LAN/MAN Standards Committee. IEEE Standard for Information Technology-Tele communication and Information Exchange between Systems-Local and Metropolitan Area Networks-Specific Requirements Part11: Wireless LAN Medium Access Control (MAC) and physical layer (PHY) Specifications Amendment1: Radio Resource Measurement of Wireless LANs. 2009.Available online:http://standards.ieee.org/getieee802/download/802.11n-2009.pdf(accessedon13July2020).

[82] Bicakci, K.; Tavli, B. Denial-of-Service attacks, and countermeasures in IEEE802. 11 wireless networks. Comput. Stand. Interfaces 2009, 31, 931–941.

[83] Cope, P.; Campbell, J.; Hayajneh, T.An investigation of Bluetooth security vulnerabilities. In Proceedings of the 2017 IEEE 7th Annual Computing and Communication Workshop and Conference(CCWC), Las Vegas, NV, USA,9–11 January 2017; pp. 1–7.

[84] Lanzetta, A.M.; Cope, P.; Campbell, J.; Mohd, B.J.; Hayajneh, T. Security vulnerabilities in Bluetooth technology as used in IoT. J. Sens. Actuator Netw. 2018, 7, 28.

[85] Hassan, S. S.; Bibon, S. D.; Hossain, M. S.; Atiquzzaman, M. Security threats in Bluetooth technology. Comput. Secure. 2018, 74, 308–322.

[86] Liu, Y.; Cheng, C.; Gu, T.; Jiang, T.; Li, X. A lightweight authenticated communication scheme for smart grid. IEEESens. J. 2015, 16, 836–842.

[87] Singh, M. M.; Adzman, K. A. A. K.; Hassan, R. Near Field Communication(NFC) Technology Security Vulnerabilities and Countermeasures. Int. J. Eng. Technol. 2018, 7, 298–305.

[88] Roland, M.; Langer, J.; Scharinger, J. Security vulnerabilities of the NDEF signature record type. In Proceedings of the 2011 Third International Workshop on Near Field Communication, Hagenberg, Austria, 22 February 2011; pp. 65–70.

[89] Amin, Y. M.; Abdel-Hamid, A. T. A comprehensive taxonomy and analysis of IEEE 802.15.4 attacks. J. Electr. Comput. Eng. 2016, 2016, 4.

[90] Amin, Y. M.; Abdel-Hamid, A.T. Classification and analysis of IEEE 802.15. 4 PHY layer attacks. In Proceedings of the 2016 International Conference on Selected Topics in Mobile & Wireless Networking(MoWNeT), Cairo, Egypt, 11–13 April 2016; pp.1–8.

[91] Amin, Y.M.; Abdel-Hamid, A.T. Classification and analysis of IEEE 802.15. 4 MAC layer attacks. In Proceedings of the 2015 11th International Conference on Innovations in Information Technology(IIT), Dubai, United Arab Emirates, 1–3 November 2015; pp.74–79.

[92] Mayzaud, A.; Badonnel, R.; Chrisment, I. A Taxonomy of Attacks in RPL-based Internet of Things. Int. J. Netw. Secure. 2016, 18, 459–473.

[93] Cao, Z.; Hu, J.; Chen, Z.; Xu, M.; Zhou, X. Feedback: Towards dynamic behavior and secure routing for wireless sensor networks. In Proceedings of the 20th International Conference on Advanced Information Networking and Applications(AINA'06), Vienna, Austria,18–20 April 2006; Volume 2, pp. 160–164.

[94] Sen, J. Security in wireless sensor networks. Wireless.Sens. Netw. Curr. Status Future Trends 2012, 407, 53–57.

[95] Hummen, R.; Hiller, J.; Wirtz, H.; Henze, M.; Shafagh, H.; Wehrle, K. 6LoWPAN fragmentation attacks andmitigation mechanisms. In Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, Budapest, Hungary, 17–19 April 2013; pp. 55–66.

[96] Vacca, J. R.Computer and Information Security Handbook; Steve Elliot: Sydney, Australia,2012.

[97] Keshk, M.; Turnbull, B.; Moustafa, N.; Vatsalan, D.; Choo, K. K. R. A Privacy-Preserving Framework based Blockchain and Deep Learning for Protecting Smart Power Networks. IEEE Trans. Ind. Inf. 2020,16, 5110–5118.

[98] Liu, C.; Yang, J.; Chen, R.; Zhang, Y.; Zeng, J. Research on immunity-based intrusion detection technology for the internet of things. In Proceedings of the 2011 Seventh International Conference on Natural Computation, Shanghai, China,26–28 July 2011; Volume1, pp.212–216.

[99] Kasinathan, P.; Pastrone, C.; Spirito, M.A.; Vinkovits, M. Denial-of-Service detection in 6LoWPAN based Internet of Things. In Proceedings of the 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications(WiMob), Lyon, France, 7–9 October 2013; pp. 600–607.

[100] Kasinathan, P.; Costamagna, G.; Khaleel, H.; Pastrone, C.; Spirito, M.A. An IDS framework for the internet of things empowered by 6LoWPAN. In Proceedings of the 2013 ACM SIGSAC Conference on Computer &CommunicationsSecurity, Berlin, Germany,4–8 November 2013; pp. 1337–1340.

[101] Oh, D.; Kim, D.; Ro, W. A malicious pattern detection engine for embedded security systems in the Internet of Things. Sensors 2014,14,24188–24211.

[102] Keshk, M.; Moustafa, N.; Sitnikova, E.; Turnbull, B.Privacy-preserving big data analytics for cyber-physical systems.WirelessNetw. 2018, 2018, 1–9, doi:10.1007/s11276-018-01912-5.

[103] Debar, H. An introduction to intrusion-detection systems.Proc.Connect2000,2000.

[104] Scarfone, K.; Mell, P. Guide to Intrusion Detection and Prevention Systems(IDPs); Technical report; National Institute of Standards and Technology: Gaithersburg, MA, USA,2012.

[105] Amaral, J.P.; Oliveira, L.M.; Rodrigues, J.J.; Han, G.; Shu, L. Policy and network-based intrusion detection system for IPv6-enabled wireless sensor networks. In Proceedings of the 2014 IEEE International Conference on Communications(ICC), Sydney, NSW, Australia,10–14 June 2014; pp. 1796–1801.

[106] Raza, S.; Wallgren, L.; Voigt, T. SVELTE: Real-time intrusion detection in the Internet of Things. Ad Hoc Netw. 2013, 11, 2661–2674.

[107] D'Agostini, G. A multidimensional unfolding method based on Bayes' theorem.Nucl. Instrum. Methods Phys. Res. Sect. accel. Spectrometers Detect. Assoc. Equip. 1995, 362, 487–498.

[108] Panda, M.; Patra, M. R. Network intrusion detection using naive Bayes. Int. J. Comput. Sci. Netw. Secure. 2007, pp. 258–263.

[109] Mukherjee, S.; Sharma, N. Intrusion detection using naive Bayes classifier with feature duction. ProcediaTechnol.2012,4,119–128.

[110] Agrawal, S.; Agrawal, J.Survey on anomaly detection using data mining techniques. Procedia Comput. Sci.2015,60,708–713.

[111] Swarnkar, M.; Hubballi, N. OCPAD: One class Naïve Bayes classifier for payload based anomaly detection. Expert Syst. Appl. 2016,64,330–339.

[112] Box, G.E.; Tiao, G.C. Bayesian Inference in Statistical Analysis; John Wiley & Sons: Hoboken, NJ, USA, 2011; Volume40.

[113] Ng, A.Y.; Jordan, M. I. On discriminative vs. generative classifiers: A comparison of logistic regression and naive Bayes. Advances in Neural Information Processing Systems; 2002; pp. 841–848. Available online: https://ai.stanford.edu/~ang/papers/nips01-discriminativegenerative.pdf (accessedon13July2020).

[114] Soucy, P.; Mineau, G.W. A simple KNN algorithm for text categorization. In Proceedings of the2001 IEEE International Conference on Data Mining, SanJose, CA, USA, 29 November–2 December 2001; pp. 647–648.

[115] Deng, Z.; Zhu, X.; Cheng, D.; Zong, M.; Zhang, S. Efficient kNN classification algorithm for big data. Neurocomputing 2016, 195, 143–148.

[116] Adetunmbi, A.O.; Falaki, S.O.; Adewale, O.S.; Alese, B.K. Network intrusion detection is based on a rough set and k-nearest neighbor.Int.J.Comput.ICTRes.2008, 2,60–66.

[117] Li, L.; Zhang, H.; Peng, H.; Yang, Y. Nearest neighbors based density peaks approach to intrusion detection. Chaos Solitons Fractals 2018,110, 33–40.

[118] Su, M. Y. Real-time anomaly detection systems for Denial-of-Service attacks by weighted k-nearest-neighbor classifiers. ExpertSyst. Appl. 2011, 38, 3492–3498.

[119] Pajouh, H. H.; Javidan, R.; Khatami, R.; Ali, D.; Choo, K. K. R. A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks. IEEE Trans. Emerg. Top. Comput. 2016, doi: 10.1109/TETC. 2016.2633228.

[120] Li, W.; Yi, P.; Wu, Y.; Pan, L.; Li, J. A new intrusion detection system based on the KNN classification algorithm in a wireless sensor network.J.Electr.Comput.Eng.2014,2014,doi:10.1155/2014/240217.

[121] Kotsiantis,S.B.;Zaharakis,I.;Pintelas,P.Supervisedmachinelearning:Areviewofclassificationtechniques.Emerg.Artif.Intell.Appl.Comput.Eng.2007,160,3–24.

[122] Du, W.; Zhan, Z. Building decision tree classifier on private data. In Proceedings of the IEEE International Conference on Privacy, Security and Data Mining; Australian Computer Society, Inc.: Sydney, NSW, Australia, 2002; Volume 14, pp. 1–8.

[123] Quinlan, J. R. Induction of decision trees. Mach. Learn. 1986, 1, 81–106.

[124] Kotsiantis, S. B. Decision trees: Are cent overview. Artif.Intell.Rev.2013,39,261–283.

[125] Goeschel, K.Reducing false positives in intrusion detection systems using data-mining techniques utilizing support vector machines, decision trees, and naive Bayes for off-line analysis. In Proceedings of the Southeast Con 2016, Norfolk, VA, USA, 30 March–3 April 2016; pp.1–6.

[126] Kim, G.; Lee, S.; Kim, S.A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Syst. Appl. 2014, 41, 1690–1700.

[127] Alharbi, S.; Rodriguez, P.; Maharaja, R.; Iyer, P.; Subas Chandra bose, N.; Ye, Z. Secure the internet of things with challenge-response authentication in fog computing. In Proceedings of the 2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC), San Diego, CA, USA, 10–12 December 2017; pp. 1–2.

[128] Tong, S.; Koller, D.Support vector machine active learning with applications to text classification. J. Mach. Learn. Res. 2001, 2, 45–66.

[129] Vapnik, V. The Nature of Statistical Learning Theory; Springer Science & Business Media: Berlin, Germany, 2013.

[130] Miranda, C.; Kaddoum, G.; Bou-Harb, E.; Garg, S.; Kaur, K. A collaborative security framework for software-defined wireless sensor networks. IEEE Trans. Inf. Forensics Secure. 2020, 15, 2602–2615.

[131] Liu, Y.; Pi, D. A novel kernel SVM algorithm with game theory for network intrusion detection. KSIITrans. Internet Inf. Syst. 2017, 11, doi:10.3837/ 2017.08.016.

[132] Hu, W.; Liao, Y.; Vemuri, V . R. Robust Support Vector Machines for Anomaly Detection in Computer Security ICMLA. 2003; pp. 168–174. Available online: https://web.cs.ucdavis.edu/~vemuri/papers/rvsm.pdf(accessedon13July2020).

[133] Wagner, C.; François, J.; Engel, T. Machine learning approach for IP-flower cord anomaly detection. In International Conference on Research in Networking; Springer: Berlin, Germany, 2011; pp.28–39.

[134] Garg, S.; Kaur, K.; Kaddoum, G.; Gagnon, F.; Kumar, N.; Han, Z. Sec-IoV: A multi-stage anomaly detection scheme for the internet of vehicles. In Proceedings of the ACM MobiHoc Workshop on Pervasive Systems in the IoT Era, Catania, Italy, 2 July 2019; pp. 37–42.

[135] Torres, J. M.; Comesaña, C. I.; García-Nieto, P. J. Machine learning techniques applied to cyber security. Int. J. Mach. Learn. Cybern. 2019, 10, 2823–2836.

[136] Ioannou, C.; Vassiliou, V. Classifying Security Attacks in IoT Networks Using Supervised Learning. In Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems(DCOSS), Santorini, Greece, 29–31 May 2019; pp. 652–658.

[137] Lin, K. C.; Chen, S. Y.; Hung, J. C. Botnet detection using support vector machines with artificial fish swarm algorithm. J. Appl. Math. 2014, 2014, doi:10.1155/2014/986428.

[138] Wozniak, M.; Graña, M.; Corchado, E. A survey of multiple classifier systems as hybrid systems. Inf. Fusion 2014, 16,3–17.

[139] Illy, P.; Kaddoum, G.; Moreira, C. M.; Kaur, K.; Garg, S. Securing fog-to-things environment using intrusion detection system based on ensemble learning. In Proceedings of the 2019 IEEE Wireless Communications and Networking Conference(WCNC), Marrakesh, Morocco,15–18 April 2019; pp. 1–7.

[140] Domingos, P. M. A few helpful things to know about machine learning. Commun. ACM2012, 55, 78–87.

[141] Zhang, H.; Liu, D.; Luo, Y.; Wang, D. Adaptive Dynamic Programming for Control: Algorithms and stability; Springer Science & Business Media: Berlin, Germany, 2012.

[142] Baba, N. M.; Makhtar, M.; Fadzli, S. A.; Awang, M. K. Current Issues in Ensemble Methods and Its Applications. J. Theor. Appl. Inf. Technol. 2015, 81, 266.

[143] Santana, L. E.; Silva, L.; Canuto, A.M.; Pinto, F.; Vale, K. O. A comparative analysis of genetic algorithm and ant colony optimization to select attributes for a heterogeneous ensemble of classifiers. In Proceedings of the IEEE Congress on Evolutionary Computation, Barcelona, Spain, 18–23 July 2010; pp.1–8.

[144] Aburomman, A. A.; Reaz, M. B. I. A novel SVM-kNN-PSO ensemble method for intrusion detection system. Appl. Soft Comput. 2016, 38, 360–372.

[145] Gaikwad, D.; School, R.C. Intrusion detection system using bagging ensemble method of machine learning. In Proceedings of the 2015 International Conference on Computing Communication Control and Automation, Pune, India,26–27 February 2015; pp. 291–295.

[146] Reddy, R. R.; Ramadevi, Y.; Sunitha, K. Enhanced anomaly detection using ensemble support vector machine. In Proceedings of the 2017 International Conference on Big Data Analytics and Computational Intelligence(ICBDAC), Chirala, India, 23–25 March2017; pp.107–111.

[147] Bosman, H. H.; Iacocca, G.; Tejada, A.; Wörtche, H. J.; Liotta, A. Ensembles of incremental learners to detect anomalies in Adhoc sensor networks. AdHoc Netw. 2015, 35, 14–36.

[148] Breiman, L. Random forests. Mach. Learn. 2001, 45, 5–32.

[149] Cutler, D. R.; Edwards, T. C., Jr.; Beard, K. H.; Cutler, A.; Hess, K. T.; Gibson, J.; Lawler, J. J. Random forests for classification in ecology.Ecology 2007, 88, 2783–2792.

[150] Chang, Y.; Li, W.; Yang, Z. Network intrusion detection based on random forest and support vector machine. In Proceedings of the 2017 IEEE International Conference on Computational Science and Engineering (CSE)and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), Guangzhou, China, 21–24 July 2017; Volume1, pp. 635–638.

[151] Zhang, J.; Zulkernine, M. A hybrid network intrusion detection technique using random forests. In Proceedings of the first International Conference on Availability, Reliability and Security (ARES'06), Vienna, Austria,20–22 April 2006;p.8.

[152] Doshi, R.; Apthorpe, N.; Feamster, N. Machine learning DDoS detection for the consumer internet of things devices. In Proceedings of the 2018 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 24 May 2018; pp. 29–35.

[153] Meidan, Y.; Bohadana, M.; Shabtai, A.; Ochoa, M.; Tippenhauer, N.O.; Guarnizo, J.D.; Elovici, Y. Detection of unauthorized IoTdevices using machine learning techniques. arXiv2017, arXiv:1709.04647.

[154] Jain, A. K. Dataclustering: 50 years beyond K-means.Pattern Recognit. Lett. 2010, 31, 651–666.

[155] Hartigan, J. A.; Wong, M. A. Algorithm AS 136: A k-means clustering algorithm. J. R. Stat. Society. Ser. Appl. Stat.1979, 28, 100–108.

[156] Bhuyan, M. H.; Bhattacharyya, D. K.; Kalita, J. K. Network anomaly detection: Methods, systems and tools. IEEECommun. Surv. Tutor. 2013,16, 303–336.

[157] Kanjanawattana, S. A Novel Outlier Detection Applied to an Adaptive K-Means. Int. J. Mach. Learn. Comput. 2019, 9, doi:10.18178/ijmlc.2019.9.5.841.

[158] Muniyandi, A. P.; Rajeswari, R.; Rajaram, R. Network anomaly detection by cascading k-Means clustering and C4.5 decision tree algorithm. Procedia Eng. 2012, 30, 174–182.

[159] Zhao, S.; Li, W.; Zia, T.; Zomaya, A. Y. A dimension reduction model and classifier for anomaly-based intrusion detection in the 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), Orlando, FL, USA, 6–10 November 2017; pp. 836–843.

[160] Hoang, D. H.; Nguyen, H.D. Detecting Anomalous Network Traffic in IoT Networks. In Proceedings of the 2019 21st International Conference on Advanced Communication Technology(ICACT), Pyeong Chang, Korea, 17–20 February 2019; pp. 1143–1152.

[161] Hoang, D. H.; Nguyen, H. D. A PCA-based method for IoT network traffic anomaly detection. In Proceedings of the 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon-si, Korea, 11–14 February 2018; pp. 381–386.

[162] Zhang, B.; Liu, Z.; Jia, Y.; Ren, J.; Zhao, X. Network intrusion detection method based on PCA and Bayes algorithm. Secure.Commun. Netw. 2018, 2018, doi:10.1155/2018/1914980.

[163] Moustafa, N.; Turnbull, B.; Choo, K. K. R. An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. IEEE Internet Things J. 2018, 6, 4815–4830.

[164] Ahmad, A.; Dey, L.A k-mean clustering algorithm for mixed numeric and categorical data. Data Knowl. Eng. 2007, 63, 503–527.

[165] Nweke, H. F.; Teh, Y. W.; Al-Garage, M. A.; Alo, U. R. Deep learning algorithms for human activity recognition using mobile and wearable sensor networks: State of the art and research challenges. Expert Syst. Appl. 2018, 105, 233–261.

[166] DeConinck, E.; Verbelen, T.; Vankeirsbilck, B.; Bohez, S.; Simoens, P.; Demeester, P.; Dhoedt, B. Distributed neural networks for Internet of Things: The Big-Little approach. In International Internet of Things Summit; Springer: Berlin, Germany, 2015; pp.484–492.

[167] Yousefi-Azar, M.; Varadharajan, V.; Hamey, L.; Tupakula, U.Autoencoder-based feature learning for cyber security applications. In Proceedings of the 2017 International Joint Conference on Neural Networks(IJCNN), Anchorage, AK, USA,14–19 May 2017; pp.3854–3861.

[168] Hinton,G. E. A practical guide to training restricted Boltzmann machines. In Neural Networks: Tricks of the Trade; Springer: Berlin, Germany, 2012; pp. 599–619.

[169] Hiromoto, R. E.; Haney, M.; Vakanski. A secure architecture for IoT with supply chain risk management. In Proceedings of the2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications(IDAACS), Bucharest, Romania, 21–23 September 2017; Volume1, pp. 431–435.

[170] Zhang, Q.; Yang, L. T.; Chen, Z.; Li, P.A survey on deep learning for big data. Inf. Fusion 2018, 42, 146–157.

[171] Li, H.; Ota, K.; Dong, M. Learning IoT inedge: Deep learning for the Internet of Things with edge computing. IEEE Netw. 2018, 32, 96–101.

[172] Fadlullah, Z. M.; Tang, F.; Mao, B.; Kato, N.; Akashi, O.; Inoue, T.; Mizutani, K. State-of-the-art deep learning: Evolving machine intelligence toward tomorrow’s intelligent network traffic control systems. IEEE Commun.Surv. Tutor. 2017, 19, 2432–2455.

[173] LeCun, Y.; Bengio, Y.; Hinton, G. Deep learning. Nature 2015, 521, 436–444.

[174] Hermans, M.; Schrauwen, B.Training and analysing deep recurrent neural networks. Adv. Neural Inf. Process. Syst. 2013, 26, 190–198.

[175] Pascanu, R.; Gulcehre, C.; Cho, K.; Bengio, Y. How to construct deep recurrent neural networks. arXiv2013, arXiv:1312.6026.

[176] Torres, P.; Catania, C.; Garcia, S.; Garino, C. G. An analysis of recurrent neural networks for botnet detection behaviour. In Proceedings of the 2016 IEEE biennial congress of Argentina (ARGENCON), Buenos Aires, Argentina, 15–17 June 2016; pp. 1–6.

[177] Armani, M.; Abu Ghazleh, A.; Al-Rahayfeh, A.; Altieri, S.; Razaque, A. Deep recurrent neural network for IoT intrusion detection system. Simul. Model. Pract. Theory 2019, 101, 102031.

[178] Guo, T.;Xu, Z.; Yao, X.; Chen, H.; Aberer, K.; Funaya, K. Robust Online Time Series Prediction with Recurrent Neural Networks. In Proceedings of the 3Rd IEEE/Acm International Conference on Data Science and Advanced Analytics, (Dsaa2016), Montreal, QC, Canada, 17–19 October 2016; pp. 816–825.

[179] Qin, Y.; Song, D.; Chen, H.; Cheng, W.; Jiang, G.; Cottrell, G. A dual-stage attention-based recurrent neural network for time series prediction. arXiv2017, arXiv:1704.02971.

[180] Malhotra, P.; Vig, L.; Shroff, G.; Agarwal, P.Long Short Term Memory Networks for Anomaly Detection in Time Series; Presses Universitaires deLouvain: Louvain-la-Neuve, Belgium, 2015; Volume89, pp.89–94.

[181] Shipman, D. T.; Gurevitch, J. M.; Piselli, P. M.; Edwards, S. T. Time series anomaly detection; detection of anomalous drops with limited features and sparse examples in noisy highly periodic data.arXiv2017, arXiv:1708.03665.

[182] Bontemps, L.; McDermott, J.; Le-Khac, N. A. Collective anomaly detection is based on long short-term memory recurrent neural networks. In International Conference on Future Data and Security Engineering; Springer: Berlin, Germany, 2016; pp. 141–152.

[183] Zhu, L.; Laptev, N. Deep and confident prediction for time series at uber. In Proceedings of the 2017 IEEE International Conference on Data Mining Workshops(ICDMW), New Or leans, LA, USA, 18–21 November 2017; pp.103–110.

[184] Goodfellow, I.; Bengio, Y.; Courville, A Deep Learning; The MITPress: Cambridge, MA, USA, 2016.

[185] Chen, X .W .; Lin, X. Big data deep learning: Challenges and perspectives. IEEE Access 2014, 2, 514–525.

[186] Ciresan, D. C.; Meier, U.; Masci, J.; Gambardella, L. M.; Schmidhuber, J. Flexible, higher-formance convolutional neural networks for image classification. In Proceedings of the twenty-Second International Joint Conference on Artificial Intelligence, Barcelona, Spain, 16–22 July 2011.

[187] Scherer, D.; Müller, A.; Behnke, S. Evaluation of pooling operations in convolutional architectures for object recognition. In International Conference on Artificial Neural Networks; Springer: Berlin, Germany, 2010; pp. 92–101.

[188] Chen, Y.; Zhang, Y.; Maharjan, S. Deep learning for secure mobile edge computing. arXiv2017, arXiv:1709.08025.

[189] McLaughlin, N.; Martinez del Rincon, J.; Kang, B.; Yerima, S.; Miller, P.; Sezer, S.; Safaei, Y.; Trickel, E.; Zhao, Z.; Doupé, A.; et al. Deep android malware detection. In Proceedings of the Seventh AC Mon Conference on Data and Application Security and Privacy, Scottsdale, AZ, USA, 22–24 March 2017; pp. 301–308.

[190] Wang, W.; Zhu, M.; Zeng, X.; Ye, X.; Sheng, Y. Malware traffic classification using convolutional neural network for representation learning. In Proceedings of the 2017 International Conference on Information Networking(ICOIN), DaNang, Vietnam, 11–13 January 2017; pp.712–717.

[191] Mohammadi, M.; Al-Fuqaha, A.; Sorour, S.; Guizani, M. Deep learning for IoT big data and streaming analytics: A survey. IEEE Commun. Surv. Tutor. 2018, 20, 2923–2960.

[192] Mayuranathan, M.; Murugan, M.; Dhanakoti, V. Best features based intrusion detection system by RBM model for detecting DDoS in cloud environment. J. Ambient Intell.Hum.Comput.2019, 1–11, doi:10.1007/s12652-019-01611-9.

[193] Fiore, U.; Palmieri, F.; Castiglione, A.; De Santis, A. Network anomaly detection with the restricted Boltzmann machine.Neurocomputing2013,122,13–23.

[194] Hinton, G. E.; Osindero, S.; Teh, Y. W. A fast learning algorithm for deep belief nets. Neural Comput. 2006, 18, 1527–1554.

[195] Li, Y.; Ma, R.; Jiao, R. A hybrid malicious code detection method based on deep learning. Int. J. Secur. ItsAppl.2015,9,205–216.

[196] Good fellow, I.; Pouget-Abadie, J.; Mirza, M.; Xu, B.; Warde-Farley, D.; Ozair, S.; Courville, A.; Bengio, Y. Generative adversarial nets. Adv. Neural Inf. Process. Syst. 2014, 2672–2680.

[197] Salimans, T.; Good fellow, I.; Zaremba, W.; Cheung, V.; Radford, A.; Chen, X. Improved techniques for training gans. Adv. Neural Inf. Process. Syst. 2016, 2234–2242.

[198] Kuncheva, L. I. Combining Pattern Classifiers: Methods and Algorithms; John Wiley&Sons: Hoboken, NJ, USA, 2014.

[199] Tavallaee, M.; Bagheri, E.; Lu, W.; Ghorbani, A. A. A detailed analysis of the KDD CUP 99 data set. In Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada, 8–10 July 2009; pp. 1–6.

[200] McHugh, J. Testing intrusion detection systems: Acritique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by the linco ln laboratory. ACM Trans. Inf. Syst. Secure. (TISSUE) 2000, 3, 262–294.

[201] Moustafa, N.; Slay, J. The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set.Inf. Secure. J. A Glob. Perspect. 2016, 25, 18–31.

[202] Stolfo, S. J.; Fan, W.; Lee, W.; Prodromidis, A.; Chan, P. K. Cost-based modelling for fraud and intrusion detection: Results from the JAM project. In Proceedings of the DARPA Information Survivability Conference and Exposition, DISCEX’00, Hilton Head, SC, USA, 25–27 January 2000; Volume 2, pp. 130–144.

[203] Sharafaldin, I.; Gharib, A.; Lashkari, A. H.; Ghorbani, A. A. Towards are liable intrusion detection bench mark dataset. Softw. Netw. 2018, 2018, 177–200.

[204] Shiravi, A.; Shiravi, H.; Tavallaee, M.; Ghorbani, A. A. Toward developing asystematic approach togenerate benchmark datasets for intrusion detection. Comput. Secur. 2012, 31, 357–374.

[205] Nehinbe, J. O. As imple. Method for improving intrusion detections in corporate networks. In International.Conference on Information Security and Digital Forensics; Springer: Berlin, Germany, 2009; pp.111–122.

[206] Bhuyan, M. H.; Bhattacharyya, D. K.; Kalita, J. K. Towards Generating Real-life Datasets for Network Intrusion Detection. I J Netw. Secur. 2015, 17, 683–701.

[207] Sharafaldin, I.; Lashkari, A. H.; Ghorbani, A. A. Toward Generating a New Intrusion Detection Data set and Intrusion Traffic Characterization. In Proceedings of the 4th International Conference on Information Systems Security and Privacy, ICISSP, Funchal, Portugal, 22–24 January 2018; pp. 108–116.Availableonline: https://www.scitepress.org/Papers/2018/66398/66398.pdf(accessedon13July2020).

[208] Moustafa, N.; Slay, J. UNSW-NB15: A comprehensive data set for network intrusion detection systems(UNSW-NB15 network data set). In Proceedings of the 2015 Military Communications and information systems Conference (MilCIS), Canberra, ACT, Australia, 10–12 November 2015; pp.1–6.

[209] Koroniotis, N.; Moustafa, N.; Sitnikova, E.; Turnbull, B. Towards developing realistic botnet data set in the internet of things for network forensic analytics: Bot-IoT dataset. FutureGen. Comput. Syst. 2019, 100, 779–796.

[210] Pa, Y. M. P.; Suzuki, S.; Yoshioka, K.; Matsumoto, T.; Kasama, T.; Rossow, C. IoTPOT: Analysing the rise of IoT compromises. In Proceedings of the 9th USENIX Workshop on Offensive Technologies (WOOT 15), Washington, DC, USA, 10–11 August 2015.

[211] Xiao, L.; Wan, X.; Lu, X.; Zhang, Y.; Wu, D. IoT security techniques based on machine learning: How do IoT devices use AIto enhance security? IEEE Signal Process. Mag. 2018, 35, 41–49.