Feature Extraction and Artificial Intelligence-Based Intrusion Detection model for a Secure Internet of Things Networks

Joseph Bamidele AWOTUNDE[1*|0000-0002-1020-4432|], Sanjay MISRA[2[0000-0002-3556-9331]],

[1]Department of Computer Science, University of Ilorin, Ilorin, Nigeria
[2]Department of Computer Science and Communication, Østfold University College, Halden, Norway.

awotunde.jb@unilorin.edu.ng[1], ssopam@gmail.com[2],

Abstract. Security has been a concern in recent years, especially in the Internet of Things (IoT) system environment, where security and privacy are of great importance. Our lives have significantly transformed positively with the emergence of cutting-edge technologies like big data, edge and cloud computing, artificial intelligence (AI) with the help of the Internet, coupled with the generations of symmetric and asymmetric data distribution using highly valued real-time applications. Yet, these cut-edge technologies come with daily disastrous ever-increasing cyberattacks on sensitive data in the IoT-based environment. Hence, there is a continued need for groundbreaking strengths of AI-based models to develop and implement intrusion detection systems (IDSs) to arras and mitigate these ugly cyber-threats with IoT-based systems. Therefore, this chapter discusses the security issues within IoT-based environments and the application of AI models for security and privacy in IoT-based for a secure network. The chapter proposes a hybrid AI-model framework for intrusion detection in an IoT-based environment and a case study using CIC-IDS2017and UNSW-NB15 to test the proposmodel's performance. The model performed better with an accuracy of 99.45%, with a detection rate of 99.75%. The results from the proposed model show that the classifier performs far better when compared with existing work using the same datasets, thus prove more effective in the classification of intruders and attackers on IoT-based systems.

Keywords: Security and privacy, Internet of Things, Intrusion detection systems, Artificial intelligence, Deep Learning, Cloud computing, Edge computing, Symmetric, and asymmetric data

1 Introduction

The emergence of innovative technologies like the Internet of Things with storage resources of cloud computing has resulted in the generation of big data called big data. This has led to the witness of massive data generation by humans through IoT-based devices and sensors [1], thus changing the world of businesses in various aspects and

society in general [2]. The authors in [3] argue that these cutting-edge technologies recently drive the global market with the connecting and productive big data managed by big data analytics. Hence, these infrastructures have created attractions from the business industries and the government and resulted in the illegal accessibility of these valuable and sensitive data globally [4]. But these big data in real-world applications have been categorized into asymmetric and symmetric data distribution.

The symmetric data comes from the relationship of social networks users, and the asymmetric data comes as a result of regular network traffic with the probability of dissemination of various malicious within network protocols. There are still great hidden patterns and knowledge within real-world applications, irrespective of the missing information. Hence, it resulted in an effective and efficient way of purifying various valuable patterns from these huge data generated from the IoT-based systems, and this becomes significant in such an environment [5].

These ubiquitous technologies have really impacted people's lives in respective of background, race, and every aspect of society, and these have resulted into various kinds of attacks on these pervasive technologies, and the growing dependency on the use of Internet facilities have led to a continuous risk against the nodes and protocols of the network [6]. Thus, the ubiquitous technologies need incorporated and tangible security solutions for proper security and privacy platform. The most important features of cyberspace security are confidentiality, integrity, and availability (CIA). Anything cut short of these features by negotiating the CIA or bypassing these technologies' security components is called cybercrime or network intrusion [7-8].

With the rapid growth of ubiquitous technologies and the inception of the internet, several kinds of cybercrime or attacks have grammatically evolved globally. Not minding the tireless efforts of various experts in cybersecurity developing various defense techniques, intruders have not relented and have always found a way of targeted, valuable resources by launching automated, cultured, and adaptable cyberattacks. These attackers have causes remarkable mayhem to individuals, governments, and even various businesses worldwide [9]. A report form authors of [10] have shown that by 2021 from cybersecurity over six trillion US dollar may be lost due to various cybercrimes, and these several cutting-edge attacks could have resulted to loss of billion dollar worldwide. These result from over five million cybercrimes recorded daily through computers that have been compromised, thus a whopping 1.5 trillion US dollars. Consequently, due to the intrinsic ability of Intrusion Detection Systems (IDSs) to detect an intrusion in real-time, the methodology in recent times has witnessed increasing popularity [11].

The IDS is a difficult field that deals with detecting cyber-threats such as hostile activities or policy violations on data networks by examining the information included in the data packets that have been transmitted [12]. The data packets' contents are converted into a vector of continuous and categorical variables such as size, addresses, and flags, among other things that denotes the existence of a network link. This vector can be compared to pre-registered vectors associated with normal traffic or attacks like signature-based intrusion detection (ID), looking for comparable patterns [12]. To detect attacks, the vector might be utilized as an input to statistical or machine learning classification methods.

For instance, the authors of [13] provide a good summary of the importance of security features in cloud computing platform surveillance. They also presented a three-level cloud-based IDS that employed rules to express event Calculus's definition and monitoring aspects. Additionally, the suggested technique made advantage of the hypervisor framework to focus on application supervision during runtime and facilitate automatic reconfiguring of these programs. Finally, the article claimed to have considerably enhanced the security of cloud computing. The ID is the process of measuring and reviewing events occurring in a computer system or network for evidence of intrusion [14].

Furthermore, they describe an intrusion as an attempt to circumvent a network's or computer system's security safeguards, thereby jeopardizing the system's CIA. Finally, based on network packets, network flow, system logs, and rootkit analysis, [15-16] authors define an IDS as a piece of hardware or software that monitors various malicious actions within computer systems and networks. The misused detection (knowledge or signature-based) and anomaly-based approaches are the two basic approaches of detecting intrusions within computer systems or networks. However, the hybrid-based strategy has exploded in popularity in the last decade, combining the benefits of the two ways outlined above to create a more robust and effective system [17].

There are a variety of traditional methods for ID, such as access control systems, firewalls, and encryption. These attack detection systems have some drawbacks, especially when systems are subjected to a large number of attacks, such as denial of service (DOS) attacks. Furthermore, the systems can achieve higher false positive and negative detection rates. Researchers have applied AI models for ID in recent years with the goal of boosting attack detection rates over traditional attack detection methodologies. Since simple machine learning algorithms have significant drawbacks, and security threats are on the rise. The newest versions of AI learning models are needed, especially for the selection of features and intrusion analysis. Therefore, this chapter presents the security issues within IoT-based environments and discusses the state-of-the-art AI models for ID in an IoT-based environment for a secure network. The chapter also proposes a particle swarm optimization (PSO) model to extract relevant features from the datasets, and Convolution Neural Network (CNN) was used to classify the intruder within the IoT-based environment. The proposed system can automatically perform the selection of significant features that can be used for the classification of the datasets. Hence, the major contributions of this chapter are:

(i) The chapter proposed a novel feature extraction based on PSO algorithms, and CNN was used to identify and detect an attacker within an IoT-based network. The combined algorithms were utilized to make use of their capabilities while avoiding computational overhead expenses.

(ii) The proposed system was evaluated using two widespread and recent datasets by analyzed the capture packet file within a network and using various performance metrics like accuracy, precision, recall, F1-score, and ROC, respectively.

(iii) The model was compared with the state-of-the-art methods basic of conventional AI-based models. The findings show that the model outperforms recent work that uses the same datasets.

(iv) The IDS model also achieves huge scalability with meaningful reduction of the training time and giving low probability of false alarms rate with an overall high degree of accuracy when compared with existing methods.

The remaining part of this chapter is as follows: section 2 presents the security issues in the Internet of Things environments, section 3 discusses the applications of Artificial Intelligence for security and privacy in Internet of Things systems. Section 4 presents the methodologies used, and section 5 discusses the results with a comparative analysis of the chapter. Finally, section 6 concluded the chapter.

2 The Security Issues within IoT-based Environments

Because of the growing number of services and users in IoT networks, the security of IoT systems has become a critical concern [7]. Smart things become more effective when IoT systems and smart surroundings are integrated. The consequences of IoT security flaws, on the other hand, are extremely harmful in vital smart contexts such as health and industry [18]. Applications and services will be at risk in IoT-based intelligent devices without adequate security mechanisms. Information security in IoT systems demands more research to meet these challenges [19-20]. The CIA are three fundamental security principles of applications and services in IoT-based embedded systems. IoT-based smart houses, for example, suffer security and privacy issues that cut across all layers of the IoT framework [21].

The security of IoT systems and the complexities and interoperability of IoT settings are significant impediments to the establishment of intelligent devices in the physical world [22]. Attacks on IoT networks, such as DoS or DDoS attacks, have an impact on IoT services and consequently on the services provided by embedded systems. Researchers look at the IoT's security concerns from a variety of perspectives, including the security susceptibility of IoT routing protocols [23-24]. This chapter will concentrate on IDSs for IoT-based systems, regardless of protocol.

The security vulnerabilities that arise in the various IoT layers are the source of IoT security concerns. The physical layer faces obstacles such as physical damage, hardware failure, and power limits. The network layer faces issues such as DoS assaults, sniffers, backdoor attacks, and illegal users. The application layer faces issues such as malicious code attacks, application vulnerabilities, and software flaws [25]. According to [26], any IoT system's security issues can be divided into four categories: Threats to authentication and physical security, as well as dangers to confidentiality, data integrity, and privacy.

For IoT-based users around the world, cyber security is a top priority. However, some concerns go beyond conventional cyber threats and can result in severe security breaches. Figure 1 displays the security and privacy in IoT-based systems.

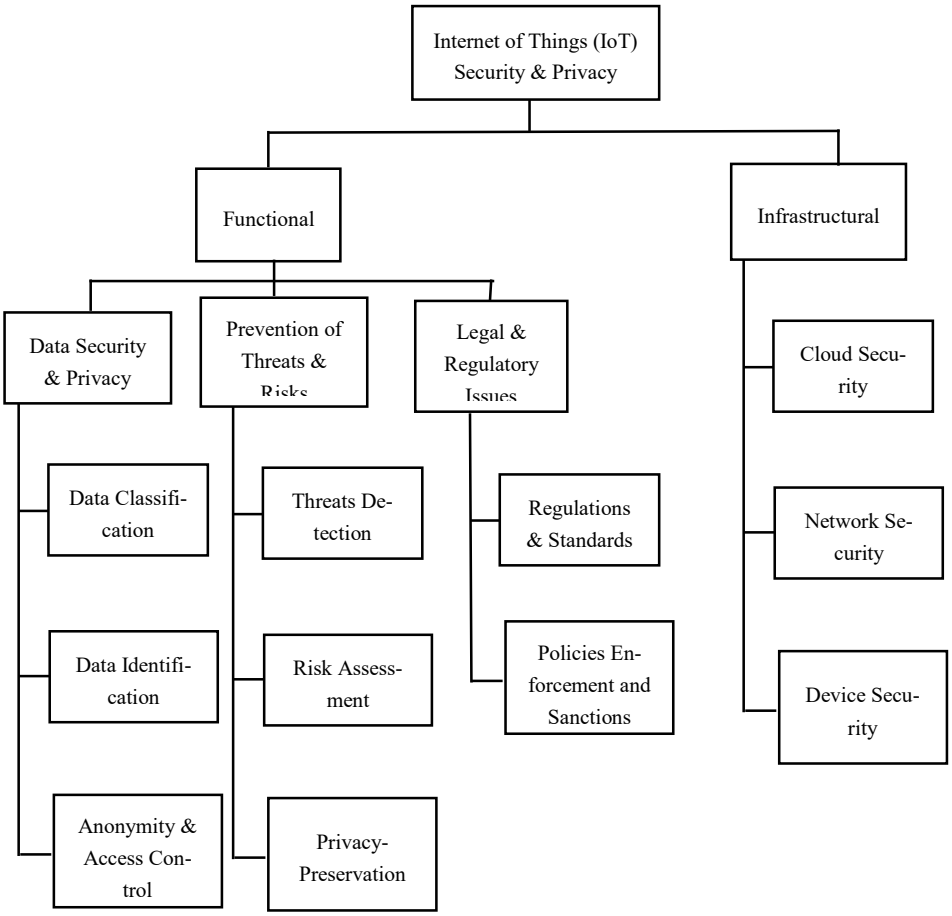

Fig. 1. The Security and Privacy in Internet of Things Systems

2.1 The following are some examples of malicious threats:

Security Problem in RFID.
The RFID system isn't without flaws. It has a wide range of applications. RFID is vulnerable to a variety of security threats and problems, all of which must be handled and addressed in WHD (wearable health care devices). Confidentiality and key management are essential. One of the most widely used techniques for automatically identifying things or individuals is radio frequency identification (RFID). The RFID application, which is based on a combination of tags and readers, is widely employed in a variety of industries, including distribution networks, engineering, and transportation control systems. Despite its many advantages, however, the technology raises a lot of hurdles and concerns, particularly in terms of security and privacy, which are deterring more researchers. RFID systems, like other devices and networks, are susceptible to

both physical and electronic attacks. As technology advances and becomes more accessible, hackers who wish to steal private information, get access to restricted areas, or bring a system down for personal benefit are becoming more common. Spying occurs when an unauthorized RFID reader listens in on conversations between a label and a reader and obtains classified information. The hacker must also understand the basic protocols, tags, and reader information in order for this technique to work.

All that is required for the assault on force research is a hacker's brain and a cell phone. According to top specialists, power analysis assaults on RFID devices can be mounted by monitoring the energy usage levels of RFID tags. When examining the power pollution levels of smart cards, researchers discovered an intrusion method, specifically the difference in supply voltages between valid and incorrect passwords. RFID tags and readers, like other goods, can be reverse-engineered; however, to get optimal performance, a thorough grasp of the protocols and features is required. Attackers will deconstruct the chip to figure out how it works in order to accept files from it.

During signal transmission, a man-in-the-middle attack occurs. Similar to eavesdropping, the attacker waits for communication between a label and a user before intercepting and modifying the data. While posing as a standard RFID component, the attacker intercepts the unique indication and then sends incorrect data. A Denial of Service attack is any RFID device malfunction that is linked to an attack. Physical attacks are widespread, including utilizing noise interference to jam the device, obstructing radio signals, and even erasing or deactivating RFID labels.

Cloning and hacking are two distinct procedures that are frequently carried out at the same time. Cloning is the process of transferring data from an original tag and applying it to a modified tag to get access to a restricted area or object. Because the intruder must know the label's details to reproduce it, this type of assault has been utilized in access control and inventory management operations. Viruses may not have adequate storage capacity in RFID tags right now, but they could represent a substantial threat to an RFID system in the future. When a virus programmed on an RFID tag by an unknown source is read at a plant, it has the potential to bring the RFID device to a halt. The virus moves from the sticker to the reader, then to corporate servers and apps, resulting in the failure of associated devices, RFID modules, and networks.

Distributed denial of service attacks (DDos).

Since the introduction of non-legacy IoT devices, DDoS attacks have become increasingly dangerous. Attackers may now use the weak security implementation of IoT devices to gain control of them and use them to launch an attack on the targeted system or network. The number of attacks has been shown to increase as the cost of adding additional IoT devices rises. A DDoS attack's principal goal is to deny legitimate users access to channel and latency facilities, resulting in service interruption [27-28]. The invader begins with non-legacy IoT systems like CCTV cameras, camcorders, baby tracking devices, and wearable gadgets, which have insufficient built-in security and other flaws, including low computational power and energy density.

IoT systems are not just difficult to attack, but they are also cheap. Attackers can obtain control of compromised IoT devices for free or at a fraction of the cost of hosting a server rather than investing in and maintaining expensive networks to launch powerful DDoS attacks. Companies do not maintain track of a device's security credentials

until after it has been released to the public. Hackers take advantage of several authentication flaws in the code. The makers do not release security fixes for these devices that correct the flawed software. If an attacker gains control of a compromised IoT device, he or she is free to change the device's security credentials. Suppose the infected computer is ever tracked for the duration of the attack. In that case, the device's vendor or manufacturer will be unable to retune the safety permits and reclaim control from the invader. The invader plans to exploit the system to cause as much harm as possible to the victim for as long as feasible.

Mobile Devices for Internet of Things Services.

Mobile devices with secure credential storage, increased storage capacity, wireless networking interfaces, and computer power can now be utilized in healthcare to collect crucial health parameters, as in Body Area Networks, and manage healthcare. The importance of privacy and protection in IoT-based systems cannot be overstated [29]. The IoT-based system's users must be aware of the potential of security vulnerabilities and information manipulation and practices becoming accessible on mobile devices as more devices and sensors become available [30]. The use of tablets and handheld devices by various users of IoT-based platforms elevates the potential of security breaches on both sides of the IoT-based settings. An intruder will install sophisticated malware in cellphones, which will remain dormant until the person in possession of the malware-infected computer enters a specific place, at which point the virus will be activated. As a result, an adversary can employ malware to tarnish a hospital's reputation by activating it whenever users of malware-infected PCs visit the facility.

IoT-based systems are becoming increasingly dangerous, and any disruption or abuse could result in significant financial loss or even life-threatening difficulties. Weak authentication mechanisms could allow a malicious attacker to get access to sensitive data and shut down all hospital systems. As a result, it's critical to ensure the safety of patients, linked devices, and hospital networks and make the operating ecosystem immune to such attacks [31-32].

An attacker can steal a client's medical record using a Man-in-the-Middle (MITM) attack on the communication network. This allows the intruder to quickly collect plaintext data from internet traffic and change a message. EMRs may also be obtained by the opponent using malicious software portable apps used by patients. The public uploading of the EMR on the network will jeopardize patients' privacy, especially for those who do not want their health problems publicized. Reverse technology is the process of creating things out of thin air. An attacker can use malicious software on mobile devices to interact with medical equipment and supply incorrect data through the application layer of the medical devices. Control system errors can lead to a physician making the wrong decision, which can have major ramifications for the patient's health [33-34].

Unintentional Misconduct.

IoT-based security is not always compromised by unscrupulous individuals seeking to harm others. Twelve percent of security issues in IoT systems were caused by unintended human behavior that resulted in a breach of patient data protection. These errors might range from misplacing a patient's file to malfunctioning security equipment.

They can also happen when old computers with patient data are discarded [1-2]. Hackers, network invaders, former workers, and others have the ability to steal or access information, disrupt operations, and harm systems. An intruder gains access to an IoT-based system via an external network and steals patient records in this pure technology hazard. As a result, it's an unsolved issue on the horizon (National Research Council, 1997). During an emergency, hospitals encourage doctors to shatter the glass (BTG) approach, which allows them to bypass entry authorisation. The IoT system's normal work cycle is disturbed in BTG scenarios. This BTG method permits doctors or other staff employees to abuse or divulge sensitive information about patients without their knowledge or consent. Health-care providers preserve records to protect against deliberate or inadvertent information misuse. In BTG scenarios, the new method is both preventative and unsuccessful [35-36].

Insider Abuse.

In 2013, insider misuse was responsible for 15% of all security breaches in the healthcare industry [37]. This word refers to circumstances in which firm employees steal goods or information or participate in other criminal conduct. Surprisingly, the amount of persons who work in the healthcare profession only to infiltrate the system and obtain access to patient health information stands out as an example of insider misappropriation. This information is typically stolen in order to get access to funds or commit tax fraud. Insider threats are becoming more and more of a worry for businesses. If these attacks are carried out, insiders' in-depth knowledge of security procedures and monitoring protocols puts firms in jeopardy. As a result, finding insiders is a significant task that has captivated the interest of scholars for over a decade. The authentication of the approved sensor nodes might be compromised, or the culprit could steal token or other information from the networks and start an attack on the entire system.

Detecting anomalies suggestive of unusual and malicious insider behavior [38], recognizing elements in attacks [39], and recognizing behavioral causes [39] have all been thoroughly discussed [40]. In an effort by the CMUCERT Insider Threat project, a pioneering assess insider threats age, sabotage, and intellectual property (IP) theft [41]. The study used a paradigm called System Dynamics to identify and characterize important paths, which the majority of insiders follow in a series of isolating questionable behavior and MERIT (Management and Information on the Risks of Security Breach) copies. In addition, the authors distinguish between insiders who unknowingly aid an attack or expose the IoT to unnecessary harm and stakeholders who act deliberately by breaking standards (to allow their daily activities) or becoming irresponsible (phishing targets) [42].

Insider risks occur when personnel within an IoT use their privileged access to compromise the system's security, credibility, or availability [43]. The severity of the insider threat is well acknowledged, as evidenced by numerous real-life incidents and detailed studies [38], [43-44]. We believe that in an era of IoT, where everything is a device capable of connecting, preserving, and exchanging important corporate data, the danger will become far more difficult to control for IoTs; this is a viewpoint shared by many others [45]. In some circumstances, it makes no sense to let these gadgets be "insiders"

recognize anything as having the potential for permitted entrance because standard perimeters are getting increasingly vague. As a result, it's critical to understand how to deal with the threat of insiders in IoT contexts. Regrettably, no comprehensive investigation of this threat has been conducted so far.

Data Integrity Attack.

In a Data Integrity attack, an attacker can tamper with a patient's data, further deceive the recipients by introducing inaccurate patient information, and then submit the erroneous information. Erroneous treatment, patient status, and emergency calls to specific people may all be the outcome of these threatening attacks. Data manipulation has the potential to result in a patient's death. Denial of Service (DoS) attacks are widespread at all layers of the network and can be carried out in a number of ways.

Data integrity is one of the most important security concerns in the Internet of Things since it affects both data storage and transfer. In the Internet of Things, data is constantly sent, with some of it being deposited and exchanged by third-party vendors who provide utilities to users. Throughout the life of the data, it must be kept confidential. Multiple service access interfaces may result in security issues. Data deposited in the schemes can be amended or deleted by attackers. Malicious apps, for example, could be installed and cause data loss. Smart city systems must mitigate this danger in order to assure data privacy. Data that does not meet the applicable requirements should be discarded using acceptable ways during the data lifecycle in IoT, which includes various phases. Data dependability is a serious concern because IoT-based data is robust in design and large in size [46].

Denial of Service Attack (DoS).

In a DoS attack, an intruder floods the system's data exchange with unidentified traffic, rendering services unavailable to others and preventing other nodes from transmitting data until the busy channel is recognized [47]. In a DoS assault, the attacker usually takes advantage of the activity by altering a certain number of flags in control ledges. Due to the labels in control packets, it is difficult to trace such an attack because nodes in the IEEE 802.11 standard do not counter-check everything. Patient data could be accessed in a DoS attack if there is no certification or authority to examine data [48]. The DoS assault frequently keeps the device's data channel busy, preventing any other data from reaching the network's other sensors. Data connection across networks is disrupted or unavailable as a result of DoS attacks. This type of attack puts system or healthcare facility accessibility and network operation, and sensor responsibilities in jeopardy.

The most common and easiest-to-enforce DoS attacks are on IoT networks. They are described as an incursion that can compromise the network's or systems' capacity to achieve their intended goals in a variety of ways. The Internet of Things has been heavily condemned from its beginning for the lack of attention devoted to safety issues in the design and deployment of its hardware, apps, and infrastructure parts [1-3], [7]. This sloppy approach has resulted in a slew of vulnerabilities that hackers and cybercriminals have successfully exploited to infiltrate IoT elements and utilize them for a variety of purposes, including staging Denial of Service and DoS attacks [49]. Users cannot access network facilities or data due to DoS assaults and DoS (DDoS) sharing. A DDoS

assault is defined as a DoS attack that has been compromised by several nodes. Given their often sophisticated and economically appealing exterior form, many IoT devices are built from low-cost generic hardware parts. Security vulnerabilities are almost often built-in to these processors and software, making it impossible for owners and administrators to keep track of them. Furthermore, the wireless problem's facilities and teamwork for firmware and software updates are still immature. As a result, updating or repairing these unprotected IoT PCs is difficult.

Router Attack.

Data routing is crucial for healthcare-based systems since it enables the supply of intelligence over the internet and simplifies connection mobility in huge facilities. Routing, on the other hand, is complicated by the fact that wireless networks are transparent. In this invasion, the attacker focuses on data transferred between sensors in various wireless sensor nodes. This is because the safe transmission of medical records to the intended recipient, who could be a physician or a specialist, is the most important prerequisite of a wireless health care system. Few implementations employ multi-trust guiding in this attack, steering basic and key facts displaying patients' daily care rankings. Multi-trust guidance is critical for growing the system's incorporation district and, as a result, providing stability at the expense of complexity.

By facilitating data flow, routers play a critical role in network communications. Protocol flaws, router software oddities, and weak authentication can all be exploited by router assaults. Two types of attacks that can arise are distributed denial of service and brute force assaults. Attacks have an immediate impact on network services and business processes. The TCP protocol employs synchronization packets known as TCP/SYN packets for link requests between computers and servers. The originator's computer When an SYN flood attack occurs, a large number of TCP/SYN packets with a forged URL are sent out. The channel's destination node is unable to connect to the root because the path is unreachable. If a router is unable to verify a TCP message, it will quickly run out of resources [50]. This is a sort of denial of service since the breadth of the assault will deplete the router's resources.

A brute force attack occurs when a hacker tries to guess a password in order to gain access to a router. The invader will utilize software with a dictionary of terms to crack the password. Depending on the strength of the password and the combinations used to discover a match, the attack could take a short time if it is relatively weak. This type of attack isn't limited to business routers; if a hacker is within range of the router, it can also happen at home. Unauthorized access to routers can be gained by a dissatisfied employee who has access to the network topology, router login and password information, and knowledge of the network topology. To avoid this problem, passwords should be changed regularly, and rigorous access controls should be implemented. Routers must have robust and up-to-date software with solid configurations to decrease their vulnerability to assaults.

Select Forwarding Attack (SFA).

In order to carry out the attack, the attacker must get access to one or more sensors. As a result, community-oriented particular forwarding is the name given to this type of

forwarding. In this technique, an attacker gains access to a sensor and drops data packets, sending them to nearby sensors to arouse suspicion. This attack significantly impacts the device, especially if the sensor is located close to the base. As a result of the packet loss generated by the SF attack, pinpointing the source of packet loss can be challenging. As a result of the partial data received by the receiver, the attack is extremely dangerous to any patient or smart medical health system.

Attacking wireless communication with selective forwarding has a major impact on network efficiency and wastes substantial energy. Previous countermeasures assumed that all peers within the communication range could notice the attacker's wrongdoing. Previous techniques have struggled to accurately detect misbehaviors because smart networks require a minimum signal-to-noise ratio to adequately gather frames and because nodes incursion is unavoidable in densely spread wireless sensor networks. In a selective forwarding assault (SFA), an intruder impersonates a normal node throughout the transmission period and selectively dismisses traffic from neighboring nodes [51]. Non-critical data can be delivered properly, but vital data can be destroyed, such as information obtained from an adversary in a military application. Because it is immoral to lose confidential information in monitoring [52], it will do major harm to WSN. Detecting and isolating SFA is a major research topic in the field of WSN defense.

Sensor Attack.

Due to accidental sensor malfunction in suspicious behavior on a cellular network perpetrated by external attackers. Sensor control necessitates the usage of cellular network limits since the sensor might be exhausted and switched off. In this situation, an attacker might simply replace a malicious sensor in the network and carry out harmful activities with ease. As a result, if the patient data is not dispersed evenly among numerous sensors, the hacker has complete control over the data. As a result of the lack of a legal permission format, false data can be injected or served.

Replay Attack.

When an intruder gains unauthorized access to a computer, a reverse attack might occur. When the sender stops sending data, the attacker runs a test on the system and sends a signal to the receiver. The attacker then takes over as the primary source. The attacker's main goal in these attacks is to generate network assurance. The attacker sends a notification to the receiver that is primarily used in the validation process. A replay attack is defined as a security breach in which data is processed without authorization and then rerouted to the recipient with the intent of luring the latter into doing something illegal, such as misidentifying or authenticating themselves or a duplicate operation. Any threat has some sort of effect on the system. The most significant effects on a health monitoring system include unauthorized access, data alteration, rejection of continuous surveillance, data goal route adjustment, and data reduction.

In this type of attack, an unauthorized person gains access to the Smart Health system, captures network traffic, and transmits the message to the receiver as the original sender [53]. The attacker wants to earn the trust of the system. A replay attack is a security breach in which any data is kept without permission and then sent again to the intended recipient. By gaining unauthorized access and then stealing critical medical information, this attack might severely impact an IoT-based system [54].

3 Applications of Artificial Intelligence for Security and Privacy in Internet of Things Systems

The development of smart devices with sensing and acting capabilities has increased the IoT platform's functionality. Because so many devices are connected to the network, a tremendous amount of data is generated [59]. In an IoT world, processing and computing is a difficult problem; thus, AI and other new technologies come to the rescue to handle the IoT security challenge. As illustrated in Figure 5, IoT and AI can be used together to enhance overall analysis, productivity improvement, and overall accuracy.

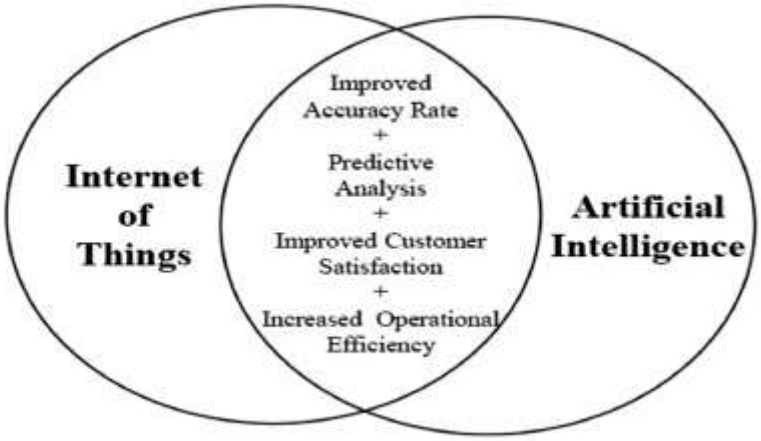

Fig. 2. The common proficiencies of IoT and AI.

Recent breakthroughs in AI may enhance the accuracy of security solutions, reducing the threats posed by the current cyberattacks [57-58]. While using AI techniques like classification and clustering is not new, their importance has lately been highlighted as AI models (e.g., deep learning) grow. Historically, the majority of AI-based security study based on predicting attack patterns and their distinctive properties. It can, nevertheless, be intrinsically vulnerable to new sorts of advanced attacks with unique properties. A recent tendency has been to apply the concept of anomaly detection to construct more generic ML algorithms to overcome this restriction of present ML systems and effective security countermeasures against unexpected assaults not identified by conventional attack patterns [60].

Most applications, such as antivirus scanners, NIS, spam detectors, and fraud detection systems could benefit from AI models. In general, such systems leverage AI models to analyze massive volumes of data generated by network traffic, host processes, and human users to identify suspicious activity [61]. There is a general belief that using AI for security applications will become commonplace in the near future. However, security solutions based on AI may be subject to a new sort of complex attack known as adversarial AI [62-63]. The adversary can effectively alter the contents of the input to AI models to circumvent classifiers designed to detect them in numerous security

domains (e.g., e-mail spam detection). Furthermore, moving normal samples to the abnormal sample class and/or vice versa could compromise the training data set used to build classifiers.

The authors in [64] demonstrated how AI might aid IoT in processing large amounts of unstructured and contradictory data in real-time, making the system more realistic. In this study [65], the authors suggest the large margin cosine estimation (LMCE) technique for detecting the adversary in IoT-enabled systems. In paper [66], the work on malware detection in IoT systems using AI is discussed. Similarly, in the article [67], the authors suggested a model for making the system tamper-proof by combining Blockchain and AI in IoT design.

The authors of [68] proposed a critical infrastructure intrusion detection system that uses an ANN classifier with backpropagation and Levenberg-Marquard features to detect abnormal network behavior. In a related effort, the authors used an ANN model for DoS/DDoS detection in IoTs in [69], and provided a decentralized IDS for IoT devices based on artificial immunity in [70]. In [71], another group of researchers introduced the Possibility Risk Identification centered Intrusion Detection System (PRI-IDS) approach to detect replay attacks using Modbus TCP/IP protocol network traffic to detect replay assaults. On the other hand, these systems had a high rate of false alarms and had difficulty detecting certain novel threats.

The authors developed IDs in wireless networks in [72], and the Aegean AWID dataset was utilized to validate the system's accuracy. A PC, two laptops, one tablet, two cellphones, and a smart TV were used to collect the AWID dataset using a SOHO 802.11 wireless network protocol. On the other hand, the collection only includes traces from the MAC layer frame and excludes IoT device telemetry data. The authors of [73] created a BoT-IoT dataset based on a realistic IoT network architecture. DDoS, DoS, service scan, keylogging, and data exfiltration are examples of attacks that include both legal and hostile traffic. The network traffic reported by the simulated IoT-based model utilizing the BoT-IoT dataset was above 72 million.

The author has provided a scaled-down version of the dataset with roughly 3.6 million records for evaluation purposes. In a similar study [74], an IoT-based dataset was employed for ADS detection in a network of IoT devices based on DoS threats. SNMP/TCMP flooding, Ping of Death, and TCP SYN flooding were used to capture data in a smart home scenario utilizing traditional and DoS assaults. However, because the dataset was not taken using an IoT-based device, it was free of XSS-Cross-site-site Scripting and malware threats. Reference [75] proposed Deep RNN for IOT IDS, which included a traffic analysis engine and categorization. The pieces of traffic information are preprocessed in a format that can be processed. Finally, a backpropagation algorithm is used to train the deep NN classifier. The classifier is divided into two categories based on system traffic: normal and attack, and an alarm is triggered if an attack is identified.

4 Methods and Materials

4.1 Particle Swarm Optimization (PSO) Model for Feature Extraction

The algorithm is an evolutionary model inspired by the predatory of birds' behaviors and was proposed [76]. The process of findings optimal fitness solutions for particles can be mimic using the methods of birds finding foods. The local optimal fitness value and the current best global fitness value of particles without knowing the optimal fitness value can provide the speed of motion for each particle. This provides the overall particle swarm to move in the direction of the best possible solution.

The two parameters of each particle can be mathematically represented by

The position is denoted by

$$x_i^k = \left[x_{i1}^k, x_{i2}^k, x_{i3}^k, \dots, x_{id}^k\right] \quad (1)$$

And the velocity by

$$x_v^k = \left[v_{i1}^k, v_{i2}^k, v_{i3}^k, \dots, v_{id}^k\right] \quad (2)$$

The position and velocity transform during the iteration update formula of each particle to:

$$v_{id}^{k+1} = \omega v_{id}^k + c_1 r_1\left(pbest_{id} - x_{id}^k\right) + c_2 r_2\left(gbest_{id} - x_{id}^k\right) \quad (3)$$

$$x_{id}^{k+1} = x_{id}^k + v_{id}^{k+1}, \quad (4)$$

where the local optimal position is represented by $pbest_{id}$ of the i^{-th} , the global optimal of all particles in the population is represented by $gbest_{id}$, ω is the inertia weight, k the number of the current iteration, v_{id}^{k+1} is the d^{-th} part of the velocity of the i^{-th} particle of k iteration, c_1 and c_2 represented the cognitive and social parameters called acceleration coefficients, r_1 and r_2 uniformly distributed over the interval [0, 1] are two random numbers, the d^{-th} component of the position of the i^{-th} particle is represented by x_{id}^{k+1} particle in the $k+1$ iteration, and the velocity of the i^{-th} particle in the k iteration of the d^{-th} the component is represented by the x_{id}^k .

Particles can readily escape the current local ideal value when the inertia weight is too great, but they are not directly coupled in the final iteration. When the inertia weight is too low, the particles, on the other hand, are easily sucked into the local ideal value. Therefore, it is necessary to adjust the inertia weight adaptively. Hence, a dynamic inertia weight called the APSO algorithm is introduced. This model was used to adjusts the inertia weight adaptively with the fitness values. The algorithm can be represented mathematically as follows:

$$\omega = \begin{cases} \omega_{min} - (\omega_{max} - \omega_{min}) * \frac{(f_{cur} - f_{min})}{(f_{avg} - f_{min})}, f_{cur} \le f_{avg}, \\ \omega_{max}, f_{cur} > f_{avg}, \end{cases} \quad (5)$$

Where the current particle fitness value is represented by f_{cur}, the current population average fitness value is represented by f_{avg}, and the smallest particles fitness values represented by f_{min} in the current population.

4.2 The Convolutional Neural Network Algorithm

The newest version of neural network with a multi-layer structure is called CNN composed of the various two-dimensional plane in each layer of the network [77-78]. To

activate the weighted sum of the elements in the previous layer, the output of each neuron is obtained.

The $C1$ layer can be represented by $C1_{ij}^{out}$ given output of the j^{-th}neuron on the i^{-th} feature plane can be mathematically given as:

$$C1_{ij}^{out} = F\left(\sum_{i=1}^{fl\ x\ 5} w_t^{in}\ x\ f_{-raw_t^{in}}\right), \quad (6)$$

Where the feature of the position of the characteristic plane is represented by $f_{-raw_t^{in}}$ corresponding to the convolution kernel weight in the input layer, w_t^{in} represents the weight of the t^{-th} position of the convolution kernel, and the length of the filter is represented by fl. Three types of nonlinear activation functions were used the sigmoid, tanh, and relu represents by $\mathrm{Fi}(\cdot)(i = 1, 2, 3)$ and can be mathematically denoted as follows:

$$F_1(x) = sigmoid(x) = \frac{1}{(1+\ exp^{-x})}, \quad (7)$$

$$F_2(x) = tanh(x) = \frac{(exp^{x} -\ exp^{-x})}{(exp^{x} +\ exp^{-x})}, \quad (8)$$

$$F_2(x) = relu(x) = max(0, x), \quad (9)$$

In the F2 layer, the output of the m-th neuron $full\ 1_m^{out}$ is as follows:

$$full\ 1_m^{out} = F\left(\sum_{n=1}^{n_{keep}} w_{min}^{keep}\ x\ keep_n +\ b_m^{f2}\right), \quad (10)$$

where b_m^{f2} is the offset of the t^{-th} neuron of the F2 layer, the connection weight between $n - th$ neurons is w_{min}^{keep} and remaining working neuron after the processing of the previous layer, and $keep_n$ is the $n - th$ neuron of the remaining working neuron.

Initially, the number of F3 neurons and activation mode is specified. In the same way that the F2 layer connects to the preceding layer, each neuron in this layer connects to the previous layer. The third and fourth layers of the fully connected layer are intended to improve learning of nonlinear combinations of compressed elements and learn the innovative functions generated by the convolution layer using the weight network connection. In the F4 layer, F3's output value is transmitted to an output layer in the last layer. The number of multi-classification task categories governs the output layer's number of neurons.

$$softmax\ (y)_i = \frac{exp^{y_i}}{\sum_{i=1}^{kind} exp^{y_i}}, \quad (11)$$

where the output value of the $i - th$ neuron is y_i in the output layer, and the number of the network attack types is represented by *kind*.

4.3 The CIC-IDS2017dataset characteristics

The Canadian Institute for Cybersecurity has released the CIC-IDS2017 dataset [79], which is unique, complex, and exhaustive, meeting the eleven most important criteria. For example, attack diversity, which includes 80 network velocity components, is a broad feature set and the necessary processes for compiling an accurate and consistent benchmark dataset. Furthermore, the authors cleverly structured the dataset to collect network traffic for five days, from Monday to Friday, which includes innocuous activity on Monday, but not on Tuesday, Wednesday, or Thursday. The first day is considered normal, and the next days are filled with cutting-edge attack traffic like DDoS, Brute Force, Heart-bleed, and Infiltration. Finally, taking into account the whole computational complexity of the CIC-IDS2017 dataset, a subset of this dataset was created

by selecting 565,053 instances at random for testing purposes. Table 1 provides the statistical summary of the CIC-IDS2017 dataset.

Table 1. The detailed summary of the CIC-IDS2017 dataset

Classes	Instances	Training set	Testing set
DDoS	60,477	42335	18,142
DoS	111,082	77,757	33,325
Botnet	1,504	1,053	451
Probe	67,929	47,550	20,379
SSH_Patator	4,715	3,301	1,414
FTP_Patator	6,348	4,444	1,904
Web Attack	4,743	3,320	1,423
Normal	990,814	693,570	297,244
Total	1,247,612	873,328	374,284

4.4 Performance analysis

The proposed hybrid model was evaluated using various metric performances and compared to other current models using the same dataset with the following performance metrics like accuracy, precision, recall, F1-score. To solve the confusion matrix, the statistical indices true positive (TP), true negative (TN), false positive (FP), and false-negative (FN) were generated, as indicated in equation (12 – (25).

Accuracy: $\frac{TP+TN}{TP+FP+FN+TN}$ (12)

Precision: $\frac{TP}{TP+FP}$ (13)

Sensitivity or Recall: $\frac{TP}{TP+FN}$ (14)

Specificity: $\frac{TN}{TN+FP}$ (15)

F1-score: $\frac{2*Precision*Recall}{Precision+Recall}$ (16)

TPR = $\frac{TP}{TP+FN}$ (17)

FPR = $\frac{FP}{FP+TN}$ (18)

5 Results and Discussion

The CIC-IDS 2017 dataset was used to test the effectiveness of the proposed system, PSO classifier was used for features extraction to reduce the features of the dataset to only the most relevant attributes, and CNN was used to classified the attack on the dataset. The PSO was used for dimensionality reduction and reduced the features to 11

relevant features. The total number of instances in the dataset is 1,247,612, and this was divided to 70%(873,328) training and 30%(374,284) testing due to the huge amount of data involved, thus help to work with reduced numbers of instances on the dataset. The performance of the proposed method is shown in table 2 using various metrics.

Table 2. The performance evaluation of the proposed model

Models	Accuracy	Sensitivity	Specificity	Precision	F1-Score	Time (Sec)
CNN	95.32	96.07	95.05	96.12	95.54	69
PSO-CNN	99.98	98.99	99.62	99.49	99.73	69

Table 2 shows the performance evaluation of the proposed model using two classes of attacks and normal, and the results show a better performance with the PSO-CNN model with an accuracy of 99.45%, the sensitivity of 98.99%, specificity of 97.62%, the precision of 98.49%, and F1-score of 99.07% with time (sec) of 69 stamps respectively. The proposed model achieved optimal results on the CIC-IDS 2017 dataset used to test the proposed model's performance for detecting intrusion. Figure 2 displays the overall performance of the proposed model PSO-CNN.

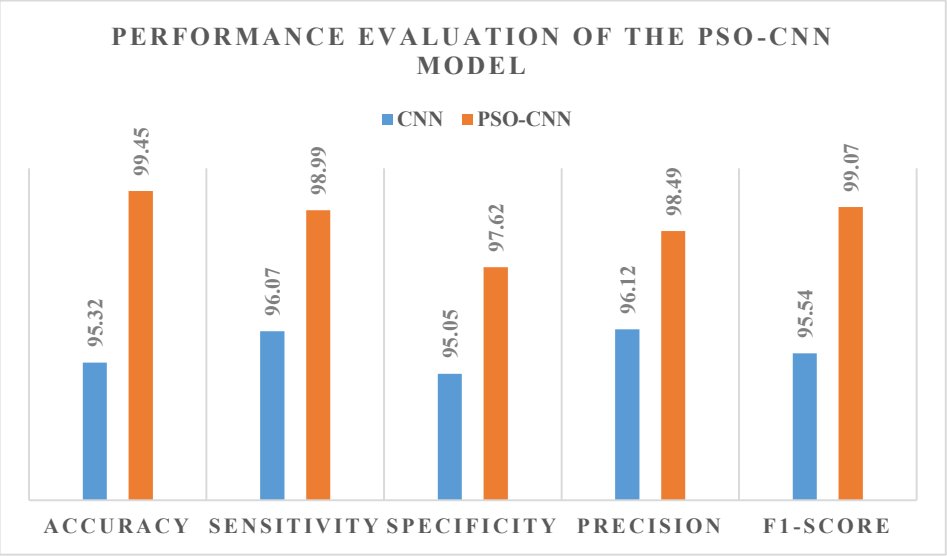

Fig. 2. The performance evaluation of PSO-CNN model

The comparison of the proposed model with the existing model

The PSO-CNN model was compared with some selected methods that used the same dataset for performance effectiveness. The two models also used different feature selection classifiers with an ensemble classifier, and the results are presented in Table 3.

The proposed model recorded a far-fetched performance in term of the metrics used for evaluation.

Table 3. The comparison of the proposed model with two existing methods using CIC-IDS 2017 datasets.

Model	Accuracy	FAR	Precision	F-Score	DR
K-Means [4]	99.72	0.011	0.992	0.992	0.997
One-Class SVM [4]	98.92	0.011	0.982	0.990	0.989
DBSCAN [4]	97.76	0.012	0.986	0.985	0.977
EM [4]	95.32	0.013	0.960	0.949	0.952
KODE [4]	99.99	0.011	0.992	0.993	0.997
CNN	98.38	0.009	0.981	0.995	0.989
Proposed Model	99.98	0.009	0.995	0.997	0.999

Table 3 shows the comparison results of the proposed model with existing classifiers, and the finding reveals that the model performs better with the results recorded. For instance, the accuracy of the proposed model is 99.98, which is almost the same as the KODE proposed by authors in [4] with 99.9% accuracy, but the model performed better in precision and F1-score with 99.49% and 99.73%, respectively. The model records a low model building time of 69 against the 217.2s in the KODE model and 0.009 false alarm rate against o.012 in the KODE model.

6 Conclusion

The loss of non-creditworthy customers has created a huge amount of loss for banks and other sectors; thus fraud detection has become useful in the financial segments. But the detection and prediction of fraud in financial sectors are very difficult due to the diversity of applicant behaviors. This study provided an intelligent model based on ANN for detecting credit and loan fraud in a highly competitive market for credit leaden limits management. ANN simplifies how banks would detect loan fraud within credit management and will make an efficient judgment in the event of a reduction in loaning supply if faced with a negative liquidity shock. Hence, concentrate on the primary goal of increasing bank profits. The results show that ANN greatly detects fraud among loan lenders and loan administrators. Therefore, the bank profit is increased by implementing the advised loan choice based on real facts. The results reveal that our proposed method outperforms other state-of-the-art methods using real transaction data from a financial institution. Future work could apply a genetic algorithm for better feature selection, which would improve the system's performance and a hybrid technique for a better result.

References

1. Awotunde, J. B., Ogundokun, R. O., & Misra, S. (2021). Cloud and IoMT-based Big Data Analytics system during COVID-19 pandemic. Internet of Things, 2021, pp. 181–201.
2. Awotunde, J. B., Adeniyi, A. E., Ogundokun, R. O., Ajamu, G. J., & Adebayo, P. O. (2021). MIoT-Based Big Data Analytics Architecture, Opportunities and Challenges for Enhanced Telemedicine Systems. *Enhanced Telemedicine and e-Health: Advanced IoT Enabled Soft Computing Framework*, 199-220.
3. Abiodun, M. K., Awotunde, J. B., Ogundokun, R. O., Adeniyi, E. A., & Arowolo, M. O. (2021). Security and Information Assurance for IoT-Based Big Data. In *Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or Opportunities* (pp. 189-211). Springer, Cham.
4. Jaw, E., & Wang, X. (2021). Feature Selection and Ensemble-Based Intrusion Detection System: An Efficient and Comprehensive Approach. *Symmetry*, *13*(10), 1764.
5. Khan, M. A., Karim, M., & Kim, Y. (2019). A scalable and hybrid intrusion detection system based on the convolutional-LSTM network. *Symmetry*, *11*(4), 583.
6. Meryem, A., & Ouahidi, B. E. (2020). Hybrid intrusion detection system using machine learning. *Network Security*, *2020*(5), 8-19.
7. Awotunde, J. B., Chakraborty, C., & Adeniyi, A. E. (2021). Intrusion Detection in Industrial Internet of Things Network-Based on Deep Learning Model with Rule-Based Feature Selection. Wireless Communications and Mobile Computing, 2021, 7154587
8. Xu, C., Shen, J., Du, X., & Zhang, F. (2018). An intrusion detection system using a deep neural network with gated recurrent units. *IEEE Access*, *6*, 48697-48707.
9. Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big data*, *7*(1), 1-29.
10. Damaševičius, R., Venčkauskas, A., Toldinas, J., & Grigaliūnas, Š. (2021). Ensemble-Based Classification Using Neural Networks and Machine Learning Models for Windows PE Malware Detection. *Electronics*, *10*(4), 485.
11. Dang, Q. V. (2019, November). Studying machine learning techniques for intrusion detection systems. In *International Conference on Future Data and Security Engineering* (pp. 411-426). Springer, Cham.
12. Lopez-Martin, M., Sanchez-Esguevillas, A., Arribas, J. I., & Carro, B. (2021). Supervised contrastive learning over prototype-label embeddings for network intrusion detection. *Information Fusion*.
13. Muñoz, A., Maña, A., & González, J. (2013). Dynamic Security Properties Monitoring Architecture for Cloud Computing. In *Security Engineering for Cloud Computing: Approaches and Tools* (pp. 1-18). IGI Global.
14. Kagara, B. N., & Siraj, M. M. (2020). A Review on Network Intrusion Detection System Using Machine Learning. *International Journal of Innovative Computing*, *10*(1).
15. Bhosale, K. S., Nenova, M., & Iliev, G. (2020). Intrusion Detection in Communication Networks Using Different Classifiers. In *Techno-Societal 2018* (pp. 19-28). Springer, Cham.
16. Liu, H., & Lang, B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey. *applied sciences*, *9*(20), 4396.
17. Saleh, A. I., Talaat, F. M., & Labib, L. M. (2019). A hybrid intrusion detection system (HIDS) based on prioritized k-nearest neighbors and optimized SVM classifiers. *Artificial Intelligence Review*, *51*(3), 403-443.

18. Awotunde, J. B., Jimoh, R. G., Folorunso, S. O., Adeniyi, E. A., Abiodun, K. M., & Banjo, O. O. (2021). Privacy and security concerns in IoT-based healthcare systems. Internet of Things, 2021, pp. 105–134.
19. Weber, M., & Boban, M. (2016, May). Security challenges of the internet of things. In *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 638-643). IEEE.
20. Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks*, *4*(2), 118-137.
21. Ali, B., & Awad, A. I. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. *sensors*, *18*(3), 817.
22. Bajeh, A. O., Mojeed, H. A., Ameen, A. O., Abikoye, O. C., Salihu, S. A., Abdulraheem, M., ... & Awotunde, J. B. (2021). Internet of Robotic Things: Its Domain, Methodologies, and Applications. Advances in Science, Technology and Innovation, 2021, pp. 203–217.
23. Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the internet of things: a survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials*, *17*(3), 1294-1312.
24. Görmüş, S., Aydın, H., & Ulutaş, G. (2018). Security for the internet of things: a survey of existing mechanisms, protocols and open research issues. *Journal of the Faculty of Engineering and Architecture of Gazi University*, *33*(4), 1247-1272.
25. Kumar, S. A., Vealey, T., & Srivastava, H. (2016, January). Security in internet of things: Challenges, solutions and future directions. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 5772-5781). IEEE.
26. Liu, X., Zhao, M., Li, S., Zhang, F., & Trappe, W. (2017). A security framework for the internet of things in the future internet architecture. *Future Internet*, *9*(3), 27.
27. Bhardwaj, A., Mangat, V., Vig, R., Halder, S., & Conti, M. (2021). Distributed denial of service attacks in cloud: State-of-the-art of scientific and commercial solutions. Computer Science Review, 39, 100332.
28. Bhati, A., Bouras, A., Qidwai, U. A., & Belhi, A. (2020, July). Deep learning based identification of DDoS attacks in industrial application. In 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4) (pp. 190-196). IEEE.
29. Taha, A. E. M., Rashwan, A. M., & Hassanein, H. S. (2020). Secure Communications for Resource-Constrained IoT Devices. *Sensors*, *20*(13), 3637.
30. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, *88*, 10-28.
31. Thomasian, N. M., & Adashi, E. Y. (2021). Cybersecurity in the Internet of Medical Things. *Health Policy and Technology*, 100549.
32. Alsubaei, F., Abuhussein, A., Shandilya, V., & Shiva, S. (2019). IoMT-SAF: Internet of medical things security assessment framework. *Internet of Things*, *8*, 100123.
33. Hyman, W. A. (2018). Errors in the use of medical equipment. In *Human error in medicine* (pp. 327-347). CRC Press.
34. Royce, C. S., Hayes, M. M., & Schwartzstein, R. M. (2019). Teaching critical thinking: a case for instruction in cognitive biases to reduce diagnostic errors and improve patient safety. *Academic Medicine*, *94*(2), 187-194.
35. Satyanaga, A., Kim, Y., Hamdany, A. H., Nistor, M. M., Sham, A. W. L., & Rahardjo, H. (2021). Preventive measures for rainfall-induced slope failures in Singapore. In *Climate and Land Use Impacts on Natural and Artificial Systems* (pp. 205-223). Elsevier.
36. Hao, F., Xiao, Q., & Chon, K. (2020). COVID-19 and China's hotel industry: Impacts, a disaster management framework, and post-pandemic agenda. *International journal of hospitality management*, *90*, 102636.

37. Chernyshev, M., Zeadally, S., & Baig, Z. (2019). Healthcare data breaches: Implications for digital forensic readiness. Journal of medical systems, 43(1), 1-12.
38. Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud). Addison-Wesley.
39. Maasberg, M., Zhang, X., Ko, M., Miller, S. R., & Beebe, N. L. (2020). An Analysis of Motive and Observable Behavioral Indicators Associated With Insider Cyber-Sabotage and Other Attacks. IEEE Engineering Management Review, 48(2), 151-165.
40. Cotenescu, V., & Eftimie, S. (2017). Insider threat detection and mitigation techniques. Scientific Bulletin "Mircea Cel Batran" Naval Academy, 20(1), 552.
41. Glancy, F., Biros, D. P., Liang, N., & Luse, A. (2020). Classification of malicious insiders and the association of the forms of attacks. Journal of Criminal Psychology.
42. Yuan, S., & Wu, X. (2021). Deep learning for insider threat detection: Review, challenges and opportunities. Computers & Security, 102221.
43. Nurse, J. R., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R., & Whitty, M. (2014, May). Understanding insider threat: A framework for characterising attacks. In 2014 IEEE Security and Privacy Workshops (pp. 214-228). IEEE.
44. Sarkar, K. R. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. information security technical report, 15(3), 112-133.
45. Nurse, J. R., Erola, A., Agrafiotis, I., Goldsmith, M., & Creese, S. (2015, September). Smart insiders: exploring the threat from insiders using the internet-of-things. In 2015 International Workshop on Secure Internet of Things (SIoT) (pp. 5-14). IEEE.
46. Altulyan, M., Yao, L., Kanhere, S. S., Wang, X., & Huang, C. (2020). A unified framework for data integrity protection in people-centric smart cities. Multimedia Tools and Applications, 79(7), 4989-5002.
47. Abdelrahman, A. M., Rodrigues, J. J., Mahmoud, M. M., Saleem, K., Das, A. K., Korotaev, V., & Kozlov, S. A. (2021). Software-defined networking security for private data center networks and clouds: Vulnerabilities, attacks, countermeasures, and solutions. International Journal of Communication Systems, 34(4), e4706.
48. Butt, S. A., Jamal, T., Azad, M. A., Ali, A., & Safa, N. S. (2019). A multivariant secure framework for smart mobile health application. Transactions on Emerging Telecommunications Technologies, e3684.
49. Ayo, F. E., Folorunso, S. O., Abayomi-Alli, A. A., Adekunle, A. O., & Awotunde, J. B. (2020). Network intrusion detection is based on deep learning model optimized with rule-based hybrid feature selection. Information Security Journal: A Global Perspective, 1-17.
50. Sivaraman, V., Venkatakrishnan, S. B., Ruan, K., Negi, P., Yang, L., Mittal, R., ... & Alizadeh, M. (2020). High throughput cryptocurrency routing in payment channel networks. In *17th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 20)* (pp. 777-796).
51. Zhang, Q., & Zhang, W. (2019). Accurate detection of selective forwarding attack in wireless sensor networks. International Journal of Distributed Sensor Networks, 15(1), 1550147718824008.
52. Liu, A., Dong, M., Ota, K., & Long, J. (2015). PHACK: An efficient scheme for selective forwarding attack detection in WSNs. Sensors, 15(12), 30942-30963.
53. Rughoobur, P., & Nagowah, L. (2017, December). A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare. In 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS) (pp. 811-817). IEEE.

54. Liu, X., Qian, C., Hatcher, W. G., Xu, H., Liao, W., & Yu, W. (2019). Secure internet of things (iot)-based smart-world critical infrastructures: Survey, case study and research opportunities. *IEEE Access*, *7*, 79523-79544.
55. Salas-Fernández, A., Crawford, B., Soto, R., & Misra, S. (2021). Metaheuristic Techniques in Attack and Defense Strategies for Cybersecurity: A Systematic Review. *Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or Opportunities*, 449-467.
56. Huseinović, A., Mrdović, S., Bicakci, K., & Uludag, S. (2020). A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid. IEEE Access, 8, 177447-177470.
57. Mosteanu, N. R. (2020). Artificial Intelligence and Cyber Security–Face To Face With Cyber Attack–A Maltese Case Of Risk Management Approach. *Ecoforum Journal*, *9*(2).
58. Singh, S., Sharma, P. K., Yoon, B., Shojafar, M., Cho, G. H., & Ra, I. H. (2020). Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. *Sustainable Cities and Society*, *63*, 102364.
59. Mohanta, B. K., Jena, D., Satapathy, U., & Patnaik, S. (2020). Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet of Things*, *11*, 100227.
60. Ogundokun, R. O., Awotunde, J. B., Misra, S., Abikoye, O. C., & Folarin, O. (2021). Application of Machine Learning for Ransomware Detection in IoT Devices. *Studies in Computational Intelligence*, 2021, 972, pp. 393–420.
61. Lee, J. H., & Kim, H. (2017). Security and privacy challenges in the internet of things [security and privacy matters]. *IEEE Consumer Electronics Magazine*, *6*(3), 134-136.
62. Huang, L., Joseph, A. D., Nelson, B., Rubinstein, B. I., & Tygar, J. D. (2011, October). Adversarial machine learning. In *Proceedings of the 4th ACM workshop on Security and artificial intelligence* (pp. 43-58).
63. Vorobeychik, Y., & Kantarcioglu, M. (2018). Adversarial machine learning. *Synthesis Lectures on Artificial Intelligence and Machine Learning*, *12*(3), 1-169.
64. Ghosh, A., Chakraborty, D., & Law, A. (2018). Artificial intelligence in Internet of things. *CAAI Transactions on Intelligence Technology*, *3*(4), 208-218.
65. Wang, S., & Qiao, Z. (2019). Robust pervasive detection for adversarial samples of artificial intelligence in IoT environments. *IEEE Access*, *7*, 88693-88704.
66. Zolotukhin, M., & Hämäläinen, T. (2018, November). On artificial intelligent malware tolerant networking for iot. In *2018 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)* (pp. 1-6). IEEE.
67. Singh, S. K., Rathore, S., & Park, J. H. (2020). Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence. *Future Generation Computer Systems*, *110*, 721-743.
68. Linda, O., Vollmer, T., & Manic, M. (2009, June). Neural network-based intrusion detection system for critical infrastructures. In 2009 international joint conference on neural networks (pp. 1827-1834). IEEE.
69. Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P. L., Iorkyase, E., Tachtatzis, C., & Atkinson, R. (2016, May). Threat analysis of IoT networks using artificial neural network intrusion detection system. In 2016 International Symposium on Networks, Computers and Communications (ISNCC) (pp. 1-6). IEEE.
70. Chen, R., Liu, C. M., & Chen, C. (2012). An artificial immune-based distributed intrusion detection model for the internet of things. In Advanced materials research (Vol. 366, pp. 165-168). Trans Tech Publications Ltd.
71. Marsden, T., Moustafa, N., Sitnikova, E., & Creech, G. (2017, December). Probability risk identification based intrusion detection system for SCADA systems. In International Conference on Mobile Networks and Management (pp. 353-363). Springer, Cham.

72. Kolias, C., Kambourakis, G., Stavrou, A., & Gritzalis, S. (2015). Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset. *IEEE Communications Surveys & Tutorials*, *18*(1), 184-208.
73. Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B. (2019). Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. *Future Generation Computer Systems*, *100*, 779-796.
74. Hamza, A., Gharakheili, H. H., Benson, T. A., & Sivaraman, V. (2019, April). Detecting volumetric attacks on lot devices via sdn-based monitoring of mud activity. In *Proceedings of the 2019 ACM Symposium on SDN Research* (pp. 36-48).
75. Almiani, M., AbuGhazleh, A., Al-Rahayfeh, A., Atiewi, S., & Razaque, A. (2020). Deep recurrent neural network for IoT intrusion detection system. *Simulation Modelling Practice and Theory*, *101*, 102031.
76. Eberhart, R., & Kennedy, J. (1995, October). A new optimizer using particle swarm theory. In *MHS'95. Proceedings of the Sixth International Symposium on Micro Machine and Human Science* (pp. 39-43). Ieee.
77. Hu, F., Zhou, M., Yan, P., Li, D., Lai, W., Bian, K., & Dai, R. (2019). Identification of mine water inrush using laser-induced fluorescence spectroscopy combined with one-dimensional convolutional neural network. *RSC advances*, *9*(14), 7673-7679.
78. Awotunde, J. B., Ogundokun, R. O., Jimoh, R. G., Misra, S., & Aro, T. O. (2021). Machine Learning Algorithm for Cryptocurrencies Price Prediction. Studies in Computational Intelligence, 2021, 972, pp. 421–447.
79. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. *ICISSp*, *1*, 108-116.