Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 2 (2023)

Literature Review on Improving IoT Security Using Machine and Deep Learning Technique

[1]Raju, [2]Rajendra Kumar

Department of Computer Science

Jamia Millia Islamia (A Central University)

New Delhi, India

Abstract **:**This literature review paper discusses the concept of the Internet of Things (IoT) and its implications on various domains, highlighting the challenges and security concerns associated with its expansive scope. This review work emphasizes the need for comprehensive security solutions to address the complexities of IoT infrastructure, particularly in the context of emerging threats. Thispaper also underscores the importance of integrating security, energy efficiency, software applications, and data analytics in IoT systems. It outlines the evolving landscape of IoT security, including the vulnerabilities and potential consequences of inadequate security measures. Additionally, authors address the intersection of security and privacy concerns within Deep Learning (DL) and Machine Learning (ML), discussing various strategies such as homomorphic encryption, differential privacy, trusted execution, and secure multiparty computing. It acknowledges the computational demands of these approaches and the ongoing search for globally harmonized solutions. Finally, authors concludes by highlighting the challenges and strategies in countering adversarial attacks in DL and ML, emphasizing the effectiveness of adversarial training and the multifaceted nature of defense mechanisms.

Keywords: *Internet of Things (IoT), Deep Learning (DL), Machine Learning (ML), Data analysis, Security, Vulnerabilities, Threats*

1. Introduction

The Internet of Things (IoT) pertains to the interlinking of diverse devices like industrial systems, smart sensors, autonomous vehicles, and more [1, 2]. It's essentially a network of physical objects connected with restricted communication, computation, and storage capabilities. These objects, equipped with embedded electronics (sensors and actuators), network connectivity, and enabling software, interact to exchange, analyze, and gather data [3].

The IoT is fostering the emergence of diverse services and applications in domains such as personal healthcare, household appliances, essential agricultural infrastructure, and military contexts [1].

The expansive scope of IoT networks presents new challenges, encompassing the administration of these devices, the sheer data volume, communication, storage, processing, as well as considerations surrounding security and privacy, among other factors.The bedrock for commercializing IoT technology is built upon the assurance of security, privacy, and user satisfaction. Leveraging potent technologies like cloud computing (CC), software-defined networking (SDN), and edge computing amplifies the array of threats assailants can exploit within IoT. Consequently, overseeing security during IoT infrastructure development has grown intricate, demanding comprehensive solutions to effectively address the security hurdles [5].Amidst the surge in connected devices, upholding dynamic IoT security norms can be challenging. To ensure requisite security, solutions must adopt a holistic approach. Despite operating autonomously, many IoT devices lack human control, potentially granting unauthorized physical access [6–8].

Moreover, the IoT ecosystem introduces fresh avenues for potential attacks. These interconnected and interdependent systems create opportunities for such vulnerabilities to arise. Consequently, the security of IoT systems faces greater jeopardy compared to that of conventional computing devices. Relying on outdated computing paradigms proves ineffective for safeguarding these intricate IoT frameworks [9–11].

The landscape of IoT systems demands an immediate integration of core considerations—security, energy efficiency, IoT software applications, and data analytics—into their operations, underscoring the breadth of their applications [7]. This expansion provides an innovative avenue for interdisciplinary scholars to examine recent IoT challenges from various angles. However, the extensive and interwoven nature of IoT devices, along with the multitude of components involved in their implementation, has spawned novel security concerns. These devices' inherent characteristics introduce a range of security issues.

Furthermore, the stages of IoT generate a wealth of valuable information. Failure to securely analyze and transmit this data may result in critical privacy vulnerabilities. While employing relevant security mechanisms like authentication, encryption, application security, network security, and access control is crucial, it proves insufficient and intricate for extensive networks intertwined with numerous systems. Every facet of the IoT platform harbors innate vulnerabilities. A recent example, the "Mirai" botnet, illustrates a distinctive threat utilizing IoT systems, leading to widespread distributed denial of service (DDoS) attacks [9, 12].

Enhancing the security landscape of the IoT ecosystem necessitates the evolution of current methods. The application of cryptographic techniques to counter specific security concerns is swiftly surpassed by novel attack variants developed by malicious actors to circumvent existing countermeasures. Among these tactics, spoofed source IPs are prevalent in amplified DDoS attacks, concealing attack origins from targeted organizations' security teams. The vulnerabilities inherent in IoT systems foreshadow the potential for even more intricate and devastating assaults, akin to the Mirai incident.

Given the diverse spectrum of IoT applications and scenarios, discerning the optimal security solutions for IoT systems proves intricate. Consequently, the crux of research lies in formulating tailored security strategies suited for IoT [12, 13]. This mandate stems from the dynamic threat landscape, where attackers continually exploit emerging weaknesses, necessitating a proactive and adaptive security approach.

The road to fortified IoT security involves a multifaceted approach, integrating proactive measures to address existing vulnerabilities, anticipating future threats, and formulating robust defenses. Research efforts should converge on not just immediate remedies but on devising holistic, versatile, and scalable security frameworks that accommodate the intricate and evolving nature of IoT deployments. Through collaborative interdisciplinary endeavors, the endeavor to bolster IoT security becomes a shared mission among researchers, developers, and stakeholders to uphold the integrity, privacy, and resilience of the IoT ecosystem.

Several strategies have been proposed to navigate the intricate interplay of security and privacy concerns within Deep Learning (DL) and Machine Learning (ML). Homomorphic encryption, differential privacy, trusted execution, and secure multiparty computing are the most frequently utilized DL and ML privacy technologies. Differential privacy, for instance, shields against an adversary's inference of instances used to construct the target model. Safe multiparty computing and homomorphic encryption safeguard training and testing data, while trusted execution environments rely on hardware-based security and isolation for protecting sensitive data and training code. However, these approaches heighten computational demands, necessitating tailored approaches for different neural network types.

Globally harmonized solutions for DL and ML privacy concerns remain elusive. A plethora of security measures, categorized into input preprocessing, bolstering model resilience, and malware detection, have been suggested to counter adversarial attacks. Preprocessing aims to reduce the model's dependence on immunity through operations like image transformation, randomization, and denoising, often without extensive model updates or retraining. Reinforcing model robustness via strategies like regulation, feature denoising, adversarial training, and other techniques falls within the second category.

Despite the array of defensive mechanisms, no singular strategy comprehensively guards against adversarial scenarios. Currently, adversarial training stands as the most effective technique to counter hostile instances. Addressing poisoning attacks involves two fundamental defense methods: outlier identification, which removes anomalies, and enhancing the neural network's resilience against tainted samples.

1.1 Motivation

Deep Learning (DL) and Machine Learning (ML) prove adept for data analytics, investigating "abnormal" and "normal" IoT behaviors as devices interconnect within the IoT environment [14]. Analyzing IoT input data uncovers standard interface patterns, enabling early malicious behavior detection. Moreover, DL/ML techniques excel at spotting novel threats, including nuanced adaptations of existing ones, through insights gleaned from past attacks. Hence, IoT systems must transition to secure communication, integrating security-driven intelligence and ML/DL methods for robust, safe, and efficient operations. This symbiotic approach fortifies IoT systems against evolving threats while optimizing their overall performance, aligning advanced data-driven strategies with the complexities of an interconnected digital landscape.

The subsequent paragraphs will delve into various distinct attributes inherent to IoT networks.

- **Heterogeneity:** Heterogeneity characterizes IoT networks, with diverse items having distinct features, protocols, and capabilities. This amalgamation enables cross-platform communication but poses challenges due to differing paradigms, protocols, and hardware constraints, adding complexity to the IoT network.

- **Proximity Communication:** IoT devices communicate autonomously, bypassing central authorities like base stations—an essential trait. Device-to-device (D2D) communication, featuring Dedicated Short Range Communication (DSRC) and other technologies, strengthens this. Decoupling services and networks fosters device-centric, content-centric communication, expanding IoT's service range beyond conventional network-centric models.

- **Massive Deployment:** The envisioned widespread deployment of IoT devices has led to predictions of the existing internet's limitations being surpassed by the billions of connected devices. However, significant challenges accompany this massive IoT expansion. These challenges encompass devising storage and network architectures for intelligent devices, optimizing data transfer protocols, and implementing proactive measures for detecting and safeguarding IoT devices against malicious attacks. The IoT's aspiration is a global communication infrastructure accessible anytime, anywhere. Connectivity varies based on the type of IoT service and application. For instance, a network of sensors or a connected vehicle may rely on local connections, while critical infrastructure management and smart home access through mobile infrastructure could demand global connectivity.

- **Cost-Effective and Energy-Efficient Communication:** The vast deployment of IoT devices requires cost-effective and ultra-low-power solutions for optimal network efficiency. For critical and modern IoT connectivity, the inclusion of self-healing and self-organizing capabilities becomes essential. Self-organizing networks are imperative in these scenarios, as reliance on fixed network structures proves inadequate.

- **Low Latency and High Reliability:** IoT networks play a pivotal role in remote surgeries, intelligent transportation, and industrial automation. Ensuring IoT's capability to swiftly and dependably respond to real-time demands is crucial for these applications.

- **Safety and Security:** The sheer volume of IoT devices connected to the internet amplifies the risk to private data exchanged through these systems. Privacy and device security are paramount concerns. The remarkable potential of IoT lies in its capacity to make informed and timely decisions based on processed data.

- **Dynamic Network Adaptation:** Effectively managing the multitude of IoT devices is a challenge. These devices exhibit dynamic behavior, with factors such as software determining sleep and wake cycles. Properly accommodating these fluctuations is imperative for efficient IoT operations.

The commercialization of IoT services and applications is intricately linked to security and privacy. Diverse sectors, including healthcare and business, have witnessed security breaches ranging from simple hacking to

sophisticated corporate-level intrusions. IoT devices and applications encounter substantial security challenges due to their constraints and operating environment. Addressing IoT security and privacy issues encompasses various perspectives, such as communication privacy and security, architecture data protection, identity management, and malware analysis [4].

Fernandes et al. [15] discuss the comparative and distinct security challenges between IoT and conventional IT devices. They also address privacy issues, with software, hardware, networks, and applications being key areas of comparison and contrast. Commonalities exist in security concerns between IoT and traditional IT. However, IoT's primary challenge lies in limited resources, hindering the implementation of advanced security measures. Addressing IoT privacy and security necessitates enhanced algorithms and cross-layer architecture. Existing security solutions, along with new intelligent, resilient, scalable, and progressive methods, will be explored to holistically manage IoT security concerns.

Machine learning (ML) involves intelligent processes that leverage past experiences or example data to enhance performance outcomes. Algorithms that employ machine learning to construct behavioral models from extensive datasets are referred to as ML algorithms. With ML, computers can learn autonomously even without explicit instructions. These models incorporate new data, serving as a basis for generating future predictions. ML has roots in AI, optimization, information theory, and cognitive science, making it a multidisciplinary domain [16].

ML finds applications in diverse areas like robotics, voice recognition, and scenarios where human intervention is challenging, such as hostile environments [12]. It proves useful when solutions evolve over time. For instance, Google employs ML to detect threats to mobile devices and apps on the Android platform, aiding in identifying and cleaning infected devices. Amazon's Macie tool utilizes ML to organize and categorize data in its cloud storage.

While ML methods are effective, they may yield false positives and true negatives. Thus, continuous direction and model adjustments are necessary to address incorrect predictions effectively.

Contrary to common perception, Deep Learning (DL), a subset of Machine Learning (ML), empowers models to ascertain their prediction accuracy. DL's self-service nature suits prediction and classification tasks in novel IoT applications, tailored with contextual support. Given the substantial data influx from IoT networks, DL and ML techniques are pivotal in rendering intelligence to these systems. Additionally, the data generated by IoT, processed through DL and ML algorithms, can inform astute decisions by IoT systems.

DL and ML offer a spectrum of applications, encompassing privacy analysis, security enhancement, malware detection, and attack prevention. DL methodologies extend to identification tasks and intricate sensing within IoT, catalyzing the creation of innovative applications and services that consider real-time interactions between individuals, the physical environment, and smart devices. The utilization of DL in IoT systems brings forth advanced capabilities, emphasizing its role in shaping the future of intelligent and responsive technology landscapes.

1.2 Contribution

The primary influences of this work are outlined as follows:

1.2.1 **Exploration of Various Attacks:** A comprehensive examination of different attack types, accompanied by illustrative examples.

1.2.2 **Analysis of IoT Defense Methods:** Thorough evaluation Deep Learning (DL) techniques for IoT security. Detailed scrutiny of promising algorithms, their advantages, drawbacks, and practical implementations.

1.2.3 **Illustration of DL :** Showcasing cutting-edge applications of DL in enhancing IoT security and privacy.

1.2.4 **Taxonomy of IoT Security Solutions:** Presenting a structured classification of recent IoT privacy and security solutions driven by deep learning. Highlighting new insights on their applications.

1.2.5 **Exploration of Future Directions:** Identifying potential limitations, challenges, and suggesting avenues for future research. Offering guidance for ongoing and forthcoming studies.

2. Literature Review

Numerous surveys and reviews have examined IoT security, providing insights into forthcoming challenges. While various studies have explored IoT security, there remains a gap in focusing on the applications of Deep Learning (DL) or Machine Learning (ML) in this domain. Prior works [19–25] have assessed challenges in access control, authentication, application security, encryption, and network security within IoT settings. A survey [26] focused on IoT communication's security concerns and corresponding solutions, while another publication [16] highlighted intrusion detection systems for IoT environments. However, a comprehensive exploration of DL and ML applications in IoT security has yet to be extensively covered.

Furthermore, regulatory and legal considerations in IoT frameworks can shape security and privacy requirements [28]. The scope of distributed IoT has also encompassed discussions on privacy and security, addressing associated challenges [29]. Researchers emphasize the benefits of the distributed IoT approach in enhancing privacy and security. In a separate survey [17], evolving threats and vulnerabilities in IoT devices, such as ransomware risks and security apprehensions, were detailed. ML techniques in the context of IoT, specifically pertaining to data security and privacy protection, were succinctly outlined in [18], which also highlighted challenges in their application, including communication overhead, partial state consideration, and backup security. Notably, surveys like [31, 32] explored data mining and ML methodologies for cybersecurity, particularly intrusion detection encompassing anomaly detection and misuse in cyberspace [19]. AI methods were analyzed within the IoT context, revealing potential applications. Another review [3] delved into ML techniques for IoT security, addressing ongoing challenges and current solutions. A survey of ML methods tailored to wireless sensor networks (WSNs) was also presented in [33].

The motivation behind this study was to review the utilization of ML techniques in real-world Wireless Sensor Network (WSN) applications, including clustering, localization, routing, quality of service (QoS) aspects, and security. Oussous et al.'s work [34] presented a framework for WSNs utilizing DL methods, primarily focusing on network configuration. This study, however, distinguishes itself by concentrating on DL/ML methods specifically aimed at enhancing IoT security. While considering both traditional ML techniques [16] and advanced approaches such as DL methods [20] for processing extensive datasets, this review particularly emphasized the relationship between various ML techniques and signal processing methodologies in the context of significant data processing.

The survey provided an in-depth view of DL in contemporary approaches [36], exploring existing solutions, their evolution, benefits, and challenges. Essential principles of diverse DL classifiers were assessed, along with their applications and advancements in fields like speech processing, pattern recognition, and computer vision [37, 22]. DL techniques' application in mobile advertising, especially recommendation systems, was highlighted [23]. Effective ML applications were similarly investigated in self-organizing networks [24]. This survey delved into the merits, demerits, opportunities, and challenges of multiple methods, contributing to the growth of artificial intelligence and future network design [41], emphasizing the significance of 5G in AI.

Intrusion detection through data mining was explored [42], and DL methods' application in multimedia mobile scenarios was surveyed [25]. Recent DL techniques in mobile security, speech recognition, mobile healthcare, language translation, and ambient intelligence were discussed. Similarly, advanced deep learning approaches within a range of IoT data analytics applications were studied [44]. In contrast, our survey provides a comprehensive overview of recent advancements in deep learning and cutting-edge machine learning approaches solely dedicated to enhancing security in the IoT domain.

This review not only compares and evaluates the strengths, potentials, and limitations of various DL/ML approaches for IoT security but also outlines future directions and challenges. By analyzing potential DL/ML applications in IoT security, the paper offers valuable insights for researchers to enhance IoT security through intelligent methods, going beyond simple secure communication between IoT modules.

3. IoT Threats

The term "IoT" refers to a network of diverse sensing systems connected via a local area network (LAN) [27]. Unique risks stem from IoT's distinctiveness, attributed mainly to the limitations of end devices [46]. Traditional internet relies on resource-rich computers and servers, unlike IoT, which employs devices with low memory and computing power. Consequently, real-world IoT devices can't employ multifactor authentication or dynamic protocols. IoT's wireless protocols, such as Zigbee and LoRa, are less secure than those of traditional networks. Varied data contents and formats within IoT applications, due to a lack of standardization and specific features, complicate creating uniform security protocols [28].

These shortcomings lead to security and privacy concerns. As networks grow, attack risks increase. IoT's absence of firewalls renders its network more vulnerable than traditional setups. Interconnected IoT systems are often multivendor, using diverse spectra and protocols, necessitating trustworthy intermediaries [48]. Concerns about app updates for countless smart devices have also arisen [49, 50]. Limited computing power hinders IoT devices' ability to handle advanced threats. IoT vulnerabilities may be intrinsic or widespread, spanning issues like battery drain attacks and insufficient standardization. Privacy and security challenges in IoT have been widely studied [32, 51–54]. This study classifies common IoT challenges over the past decade, categorizing them into privacy and protection domains.

In the Internet of Things, data comes in various forms, including user identification records and device commands. Unauthorized data disclosure breaches security, integrity, or availability, constituting a privacy threat. Both security and privacy concerns jeopardize data confidentiality and network stability. Figure 1 illustrates the variety of threats in IoT domains.

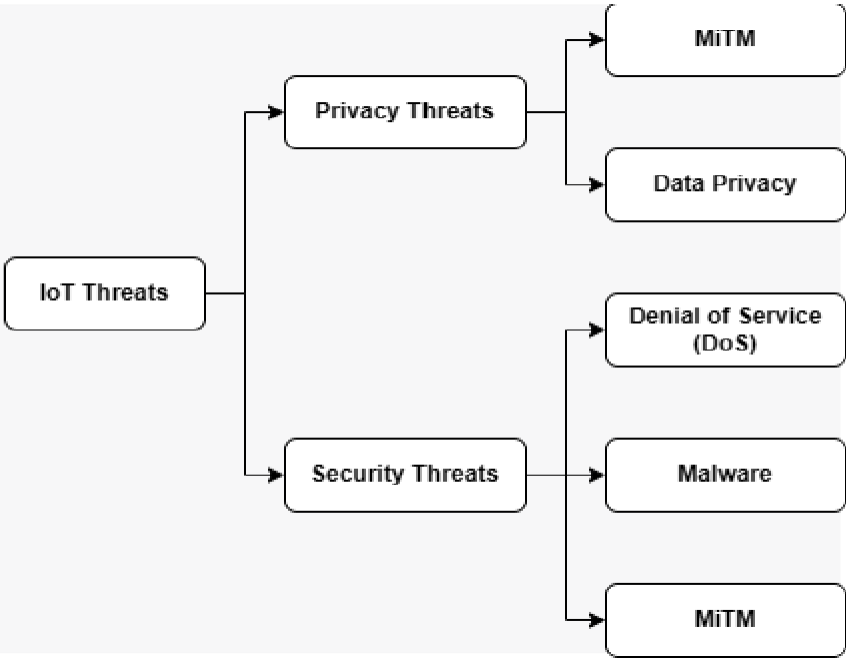

Figure 1. Type of IoT Threats

3.1 **Privacy Threats.** Beside security risks, common privacy threats in IoT encompass de-anonymization, inference, and sniffing. These threats impact data confidentiality, whether at rest or in motion. This section explores various privacy risks.

Man-in-the-Middle (MiTM) attacks include passive (PMAs) and active (AMAs) types. PMAs passively monitor data between systems without altering it. Intruders might observe for months before attacking. Passive MiTM attacks, like sniffing and eavesdropping, exploit IoT cameras. AMAs involve active misuse, such as impersonation or authorization attacks.

Data privacy encompasses passive data privacy attacks (PDPAs) and active data privacy attacks (ADPAs), paralleling MiTM attacks. Concerns include data tampering, outflow, re-identification, and identity theft. Re-identification attacks focus on recognition, de-anonymization, and aggregation, seeking to uncover targets' traits. Attackers might mimic specific objectives using gathered data. ADPAs alter records (e.g., tampering), while PDPA involves leakage and re-identification.

3.2 Security Threats

3.2.1 **Denial of Service (DoS)** attacks, though straightforward, pose a significant threat, especially with the rising number of poorly secured IoT devices. The aim is to flood the network with illicit requests, depleting resources and blocking legitimate access. Distributed Denial of Service (DDoS) attacks are more complex, targeting a specific entity from various sources. These attacks exploit protocols like SYN floods, ICMP, crossfire, and botnets, compromising IoT networks. Detection methods include applying deep learning (DL) in fog-to-things environments and using distributed DL in fog computing. Intrusion Detection Systems (IDS) employing advanced machine and deep learning algorithms can reduce DDoS attacks. Vulnerabilities in software-defined networks have also been explored [60–65].

3.2.2 **Malware** poses a significant threat to IoT systems by exploiting vulnerabilities in application security, authentication, and authorization. Attackers inject malicious code into IoT devices, often via software modifications or misconfigurations. Various forms of malware, such as spyware, adware, ransomware, and trojans, leverage these vulnerabilities. Azmoodeh et al. [39] researched malware distribution in the Internet of Battlefield Things (IoBT), often orchestrated by well-trained, well-funded hackers. Research [72–74] has utilized supervised machine learning to defend resource-constrained Android devices against malware. Studies [50, 75, 76] deeply explored malware detection, uncovering security flaws in the Android framework, particularly at the application layer with diverse component forms.

3.2.3 **Man-in-the-Middle (MiTM)** attacks, one of the earliest cyber threats [77], encompass spoofing and impersonation. Attackers intercept communications between nodes, such as 'X' and destination 'A,' exploiting vulnerabilities like SSL stripping. Recent efforts have focused on countering MiTM attacks [78–81]. Ahmad et al. [42] highlighted the vulnerability of an insulin injection system to fatal MiTM attacks. New security methods for wireless mobile devices, safeguarded keys using non-volatile memory and cryptography [44], aim to mitigate impersonation risks. OAuth 2.0, a widely used IoT protocol, is prone to cross-site request forgery attacks [44]. Researchers [45] identified a physical layer security flaw in wireless system authentication, proposing a hypothesis test to detect eavesdroppers like Eve in wireless networks, especially in active scenarios.

3.3 Another Threat to Privacy and Security.

Two primary categories of security threats exist: physical and cyber. Cyber risks are divided into active and passive subcategories. The subsequent section outlines several of these risks and threats.

3.3.1 **Physical Threats:** One type of threat involves physical destruction, often beyond the reach of a typical cyberattack due to the attacker's limited technical expertise. This implies that only physically accessible IoT devices can be affected. With the proliferation of accessible cameras and sensors, these attacks could become more prevalent as IoT deployment increases. Furthermore, natural disasters like earthquakes or human-induced crises like wars can also introduce physical threats.

3.3.2 Cyber Threats

3.3.3 **Active Threats:** An active threat involves an attacker skilled in intercepting and modifying IoT devices to manipulate settings, control communication, deny services, and more. Attacks may involve interventions, interruptions, and alterations, such as impersonation, data tampering, malicious inputs, and DoS attacks. Malicious software injection, data tampering, and denial of service attacks can compromise IoT systems, leading to severe consequences like altering smart grid billing. IoT is susceptible to various DoS attacks targeting internet or cellular connectivity, disrupting service availability [30, 85].

3.3.4 **Passive Threats:** Passive threats require eavesdropping on communication networks or channels to access sensor data. Eavesdroppers can monitor conversations and gather personal information, like health data, which has gained value in the illegal market. Eavesdropping could also reveal the location of an IoT device's owner, posing privacy risks [86]. The black market prices personal health information at $50, contrasting with credit card information at $1.50 and social security numbers at $3 [87, 88].

4. IoT Applications of Security Threat for Each Layer

This section delineates the structure of an IoT application into four tiers: sensing, network, middleware, and application layers. Each tier employs diverse technologies, posing unique security challenges. Security risks across these tiers, especially at gateways, are analyzed and discussed in this section.

4.1 **Sensing Layer and Security Concerns**. This tier is centered on IoT's physical actuators and sensors. Sensors detect nearby physical events, while actuators react based on this input. Various sensor types like video, ultrasonic, and temperature sensors are used. Security risks at the sensing layer encompass:

4.1.1 **Injection of Malicious Code Attack:** Attackers inject malicious code into IoT nodes' memory, exploiting over-the-air firmware or software updates. This may lead to unauthorized access attempts or undesired operations within the IoT system.

4.1.2 **Node Capture**: Adversaries can compromise IoT by replacing legitimate low-power nodes like actuators and sensors with malicious ones, granting attackers full control and compromising the entire application.

4.1.3 **Side-Channel Attacks (SCAs):** Adversaries exploit microarchitectures, electromagnetic emission, and power consumption to gain unauthorized access to sensitive data, leading to potential exposure through power consumption, timing, laser-based, and electromagnetic side-channel attacks.

4.1.4 **Booting Vulnerabilities:** Edge devices lack inherent security measures during startup, making them susceptible to various threats. Attackers exploit this weakness when devices are rebooted, emphasizing the need for secure startup mechanisms.

4.1.5 **Sleep Deprivation Attacks:** Attackers drain powerless IoT edge devices' battery life using malicious malware or increased power consumption, rendering them unable to function and resulting in a lack of service.

4.1.6 **False Data Injection Attack:** Compromised nodes inject false data into the IoT system, causing malfunctions. This strategy can also facilitate Distributed Denial of Service (DDoS) attacks.

4.1.7 **Eavesdropping and Interference:** IoT applications in open environments are vulnerable to eavesdropping and data theft during authentication and transmission stages, potentially leading to unauthorized data access and interference.

4.2 **Network Layer and Its Security Concerns:** The network layer facilitates data transmission from the sensor layer to the computing unit for processing. Common network security challenges include:

(i) DoS/DDoS Attack: Unwanted requests flood attacked servers, rendering them inaccessible to legitimate users. DDoS attacks use multiple sources to overwhelm a server, causing it to be unusable. IoT's complexity makes it susceptible to such attacks due to improper device configurations, as seen in the Mirai botnet attack.

(ii) Routing Attacks: Malicious nodes redirect traffic within IoT systems, potentially compromising security. Sinkhole attacks encourage nodes to follow fake routes, and wormhole attacks use unauthorized connections between nodes. An attacker may exploit vulnerabilities by creating a "wormhole" between hacked and internet-connected devices.

(iii) Access Attack: Unauthorized individuals gain IoT network access unnoticed, aiming to steal critical data. IoT's constant data collection makes it vulnerable to APTs, allowing attackers to stay hidden.

(iv) Data Transit Attacks: Valuable data face cyber threats during transit between IoT devices, sensors, and the cloud. IoT's varied connecting mechanisms can compromise data transmissions.

(v) Phishing Site Attack: Phishing targets numerous IoT devices, exploiting user credentials. Vulnerable IoT devices are targets as soon as credentials are stolen. Common in IoT's network layer

4.3 **Middleware Layer and Its Security Challenges**. In IoT, middleware acts as a bridge between the application and network layers, providing essential compute and storage capabilities [96]. APIs serve the application layer's needs, including machine learning and data storage. Yet, middleware is susceptible to attacks that risk the entire IoT application, making its security vital. Apart from database and cloud security, middleware security is crucial. Detailed descriptions of attacks on the middleware layer follow.

(i) SQL Injection Attack: Middleware can be targeted with SQL injection (SQLi), where an attacker inserts a malicious SQL query into a program, potentially accessing private user information and altering database entries [91]. SQLi is a significant web security threat, highlighted in the OWASP top 10 2018 report.

(ii) Cloud Flooding Attack: Denial of service attacks on cloud platforms, like flooding attacks, impact Quality of Service (QoS). Attackers overwhelm cloud resources with a continuous stream of queries, straining cloud servers and affecting system performance.

(iii) Man-in-the-Middle Attack: MQTT brokers act as proxies in subscriber-client communication, allowing messages to be sent to multiple recipients. An attacker gaining control over the broker can intercept all communications between subscribers and clients without their knowledge.

(iv) Signature Wrapping Attack: XML signatures in middleware's web services may be exploited through SOAP vulnerabilities in signature wrapping attacks. Attackers manipulate intercepted messages, bypassing the signature scheme and potentially performing unauthorized operations.

4.4 **Gateways and Their Security:** Gateways play a vital role in linking devices, individuals, objects, and cloud services. They facilitate IoT device hardware and software provision, handle data encryption/decryption, and protocol translation. IoT gateways support various stacks like Zigbee, LoRaWAN, TCP/IP, and Z-Wave. However, these gateways encounter security challenges, as discussed below.

4.4.1 End-to-End Encryption: Data confidentiality requires end-to-end application layer protection, ensuring only the intended recipient can decode encrypted communications. Protocols like Z-Wave and Zigbee offer encryption, but gateways are needed to decrypt and re-encrypt messages for protocol conversion. However, this decryption at the gateway level exposes data to security vulnerabilities.

4.4.2 Firmware Updates: IoT devices often lack user interfaces or computational capacity for firmware updates, typically relying on gateways. Before implementing changes, gateways should verify signature validity and compare existing and new firmware versions.

4.4.3 Extra Interfaces: Minimizing the attack surface is crucial during IoT device installation. Manufacturers should implement only essential protocols and interfaces, restricting services and functionality to end users to prevent backdoor authentication or data leaks.

4.4.4 Secure On-Boarding: Protecting encryption keys during the addition of new IoT devices is vital. Gateways serve as intermediaries between management services and new devices, making them susceptible to eavesdropping and malicious attempts to steal encryption keys during the on-boarding process.

4.5 **Application Layer and Its Security:** The application layer serves direct customer interactions in IoT, encompassing smart cities, homes, and grids. Distinct security issues like data theft and privacy arise here, unlike other levels. Diverse apps pose varying security concerns at this tier. Many IoT systems employ a middleware or application support layer between the network and application layers, offering business service support and resource management. The application layer faces critical security challenges, including data protection and privacy, which are detailed below.

4.5.1 **Reprogram Attacks:** Insecure programming of IoT devices can lead to remote reprogramming, granting complete control over the IoT [53].

4.5.2 **Malicious Code Injection:** Attackers exploit code vulnerabilities to introduce malicious scripts, potentially compromising an entire IoT system. XSS attacks are commonly used to compromise trustworthy websites, impacting the entire system upon IoT account compromise.

4.5.3 **Access Control Attacks:** Breached user credentials can jeopardize the entire IoT system by bypassing access controls.

4.5.4 **Service Interruption Attacks (DDoS):** Overloading networks or servers disrupts IoT apps, preventing legitimate users from accessing services.

4.5.5 **Data Theft:** IoT apps handle sensitive data, vulnerable due to data mobility. Encryption, isolation, and authentication methods are employed to safeguard IoT app data.

5. Deep Learning (DL) in IoT Security

Recent years have witnessed a pivotal focus on deep learning in IoT systems [14]. DL's distinct advantage over classical machine learning lies in its superior handling of vast datasets, a fitting trait for data-rich IoT schemes. DL offers dynamic data representations [55], making it an ideal partner for the interconnected IoT ecosystem [56]. Deep connection, a unified protocol, fosters automated communication between IoT devices, forming intelligent homes [14]. DL employs multi-layered computations to learn diverse abstraction levels in data structures, surpassing traditional ML methods [106, 107]. This subfield of ML leverages non-linear layers to capture hierarchical patterns, mirroring human neuron responses. Unsourced and supervised learning, even hybrid models, are integrated into deep networks. This section delves into prominent DL algorithms. Figure 5 illustrates a variety of DL classifiers designed for enhancing IoT security.

Supervised Deep Learning: This section delves into the prevalent applications of supervised DL techniques, focusing on recurrent neural networks (RNNs) and convolutional neural networks (CNNs), both prominent discriminative DL algorithms.

5.1.1 **Convolutional Neural Networks (CNNs)** were devised to reduce data parameter counts within traditional neural artificial networks (ANNs). This optimization is achieved through three key principles: sparse relationships, parameter sharing, and fair distribution [92]. Improved scalability and complexity result from diminished inter-layer connections in CNNs. Comprising convolution and pooling layers, CNNs employ analogous filters (kernels) in convolutional layers to combine data parameters [79]. Pooling layers, utilizing average or max pooling, downsize subsequent layers. The top pooling method segments input into non-overlapping clusters, selecting the highest value for each cluster from the previous layer and combining them via average pooling [94]. Another critical layer is the activation device, implementing non-linear activation functions. The ReLU (f(x) = max(0, x)) is favored for its activating node properties [79]. Figure 2 illustrates CNN operation in extended IoT security.

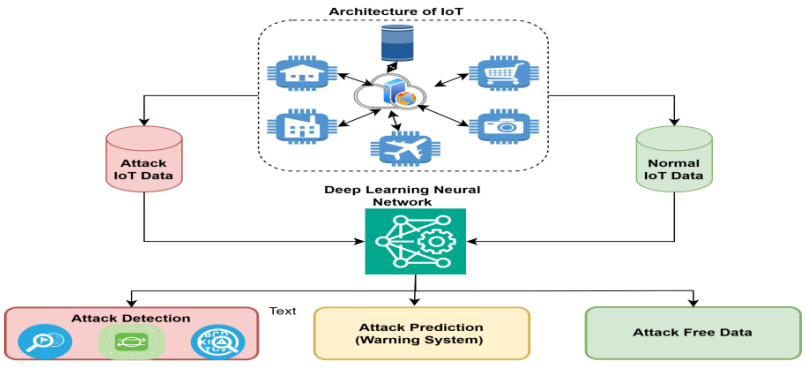

Figure 2. Deep Learning model for IoT security

Although CNNs are instrumental in deep learning approaches and excel in high-performance raw data learning, their resource-intensive nature poses challenges for deploying them on resource-constrained devices, necessitating distributed architectures. A solution is the introduction of a light deep neural network (DNN),

trained entirely within a strongly categorized neuron and equipped with a subgroup of similar output groups [58]. Primarily oriented toward image detection, CNN advancements have been pivotal in constructing accurate image ID and classification models, such as those for ImageNet.

CNNs offer value beyond image analysis, evident in a CNN-based IoT protection malware identification framework for Android. This framework utilizes CNN to extract crucial malware identification features from raw data. The advantage of CNNs lies in concurrently teaching functionality and classification, eliminating the conventional extraction step in producing comprehensive models. However, the potent learning capacity of CNNs can also be exploited by attackers, as evidenced by a study demonstrating their efficacy in breaking cryptographic applications [59].

5.1.2 **Recurrent Neural Networks (RNNs)** play a pivotal role in deep learning algorithms, especially when dealing with sequential data. RNNs are tailored for managing temporal sequences by leveraging the relationships among past instances. The current output is influenced by the interpretation of similarities between preceding examples, making the network's performance reliant on both current and past inputs. While maintaining distinct input and output layers, this design necessitates a feedforward neural network (NN) structure [60]. Initially used with the backpropagation algorithm, RNNs are ideal for tasks involving sequential inputs, such as sensor data, text, and voice recognition [61].

RNNs incorporate a sequential data storage layer along with recurrent cells housing hidden units that perpetually evolve to capture the network's ongoing state [63]. The activation of the previously hidden state informs the processing of the current hidden state. This feature enables RNNs to effectively handle sequential data, making them valuable for various tasks, including time-based threat identification. Consequently, RNNs are instrumental in strengthening neural networks and revealing significant behavioral patterns.

However, RNNs suffer from gradient vanishing or explosion issues [61]. Despite this limitation, RNNs and their derivatives have demonstrated superior performance in a range of sequential data applications, including speech recognition and translation [94]. Moreover, RNNs hold promise in enhancing IoT security. IoT networks collect vast amounts of sequential data, such as network traffic patterns, requiring robust methods to detect potential network attacks. A prior study [63] validated RNNs for network traffic analysis, effectively identifying malicious activity. RNNs offer real-world applicability, making them invaluable for safeguarding IoT systems and fortifying protection against sequential-based attacks. Advancing RNN research and its variants remains crucial for bolstering IoT security, particularly in the context of serial attacks.

5.1.3 Unsupervised Deep Learning

This section covers common unsupervised DL techniques: deep restricted Boltzmann machines (RBMs), deep belief networks (DBNs), and autoencoders (AEs) for data representation and learning.

5.1.4 **Restricted Boltzmann Machines (RBMs):** RBMs are powerful generative models. Operating in an undirected fashion, they consist of distinct visible and hidden layers. Data features are hierarchically captured, enabling subsequent layers to encode features from the previous layer [64]. RBMs hold promise for network anomaly detection [64], addressing challenges like labeled data scarcity and evolving irregular behavior. A focus on discriminatory RBMs demonstrated potential in recognizing network anomalies despite incomplete training data [64].

5.1.5 **Deep Belief Networks (DBNs):** Comprising stacked RBMs, DBNs undergo layer-wise greedy training]. Unsupervised pretraining with RBMs followed by fine-tuning enables learning hierarchical features. DBNs have excelled in diverse applications, such as malware detection [65], improving detection precision over traditional methods. In mobile edge computing security [65], DBNs outperformed manual feature engineering, demonstrating their robustness.

5.1.6 **Deep Autoencoders (AEs):** AEs, unsupervised networks, encode input to generate output [57]. They consist of an encoder and decoder [57]. AEs prioritize feature learning while handling reconstruction limitations [66]. AEs show promise in ransomware detection [66] and malware identification, outperforming traditional

machine learning algorithms [66]. Yet, AEs' effectiveness depends on data consistency between training and testing.

5.1.7 These techniques showcase deep learning's prowess in unsupervised learning scenarios, offering insights into anomaly detection, feature extraction, and data reconstruction. Their applications span network security, data analysis, and more, fueling advancements in various domains.

5.2 Semi-supervised Deep Learning

In this segment, we explore classic hybrid deep learning methods, including notable examples like Generative Adversarial Networks (GANs) and Network Communities (EDLNs).

5.2.1 **Generative Adversarial Networks (GANs):** GANs, a groundbreaking advancement introduced by Goodfellow et al. [67], stand as a compelling frontier within deep learning. Illustrated in Figure 7, GANs employ a dual model approach, simultaneously training both a generative and a discriminative model through an adversarial mechanism. The generative model captures data distribution and produces test data, while the discriminative model assesses the probability of evaluation results relative to the generative model. The generative model's training objective is to elevate its misclassification likelihood by the discriminator [95]. Each phase of GAN training involves modifying the generative model to deceive the discriminator using different sample sets. The discriminator operates as a discerning agent, distinguishing between real and synthetic samples (from training data). Through iterative refinements, the discriminator's performance aids sample generation for subsequent iterations [44].

GANs have found application in IoT security enhancement. In [68], an architecture fortified the IoT network's cybersecurity by training deep learning algorithms to differentiate normal from anomalous computational behavior. GAN algorithms were integrated into the proposed architecture for preliminary analysis, showcasing efficacy in detecting suspicious system activities [68]. GANs excel in learning diverse attack patterns, offering zero-day attack-like samples that can augment algorithms without relying solely on existing attacks. GANs are particularly adept for semi-supervised classification training, outpacing fully transparent DBNs in sample generation speed. Unlike RBMs requiring numerous Markov chain iterations, GANs only need a single sampling stage within the model [136, 139]. However, GAN training is intricate and poses challenges. Notably, GANs struggle to produce diverse data like text [95].

5.2.2 **Ensemble of DL Networks (EDLNs):** EDLNs harness hybrid generative and discriminative models, a rising trend in deep learning. Ensemble Learning (EL), an emerging algorithm, combines diverse classification approaches for performance enhancement. Homogeneous or heterogeneous multiclassifiers yield accurate outcomes, resolving various challenges. EL, although time-intensive compared to single classifiers, finds utility in anomaly, virus, and intrusion detection .

By combining DL classifiers, the EDL approach fosters model diversity, boosts performance, and extends generalization. However, a drawback lies in increased temporal complexity. Assembling numerous neural networks may lead to impractical computational costs, considering high-performance hardware training durations. Explicit/implicit ensembles address this challenge. Implicit ensembles share model parameters, approximating ensemble model averaging through a single, unthinned network at testing. In explicit ensembles, parameters aren't shared; predictions of ensemble models combine through methods like majority voting, averaging, etc.

Dropout [69] randomly deactivates hidden nodes during training, aiding regularization and sparsity. DropConnect [145], akin to Dropout, introduces sparsity in weight parameters by randomly deactivating connections. Stochastic depth [70] trims network depth during training while preserving it at testing. Swapout [148] extends Dropout and stochastic depth.

EDLNs merge generative, discriminatory, and hybrid frameworks. These stacked collections of heterogeneous or homogeneous classifiers tackle complex problems, enhancing variability, precision, and efficiency. EDLNs find success in applications like activity detection, but their application in IoT protection warrants further

investigation, particularly deploying lightweight graders in dispersed settings to augment IoT security and address machine challenges.

5.3 Deep Reinforcement Learning (DRL): Reinforcement Learning (RL) introduces an effective strategy to enhance an agent's methods by iteratively evaluating actions and adapting to achieve optimal long-term goals, devoid of prior environmental awareness. An ML subset, RL involves the agent learning action-environment interactions through trial and error, calculating rewards after each action and transitioning to the next state. RL's focus on long-term outcomes empowers it to tackle complex issues that elude traditional methods, often assuming Markovian models for real-world problems. The agent operates within states, actions, and rewards, aiming to learn policies mapping observations to actions for maximum returns.

Deep Reinforcement Learning (DRL) harnesses deep learning to address Markov decision processes (MDPs), exemplified by neural network-modeled policies like $\pi(a|s)$. DRL techniques, such as the deep Q-network (DQN) [64], have found applications in mobile edge computing, resolving high-dimensional challenges with scalability and performance. Despite its potential, DRL faces the curse of dimensionality and demands substantial data and computation.

Researchers explore DRL's synergies with other ML methods due to its limitations. For instance, in , DRL is investigated for access management, download optimization, and blockchain integration in IoT networks. In cybersecurity, DRL proves valuable, as seen in [71], where DRL-based cyber-physical security mechanisms, intrusion prevention tactics, and multi-agent cyberattack mitigation models are explored within a game theory framework. These DRL approaches hold promise within the context of IoT, advancing security and system efficiency.

6. Application of Deep Learning in IoT Security:

Deep Learning (DL) techniques have found substantial applications in enhancing the security of Internet of Things (IoT) environments. In signal authentication for IoT settings, Ferdowsi and Saad [72] introduced an LSTM architecture to derive stochastic properties from IoT device signals. Cyberattack controls were watermarked within IoT systems using complex function extraction, aiding eavesdropping attack detection. However, this centralized cloud service-based approach faces challenges in scaling to large IoT deployments.

To address scalability, LSTM-based signal authentication was combined with game theory in a mixed Nash equilibrium (NE) strategy. While dynamic and adaptable for handling many IoT modules, this solution is not optimal for IoT environments. In contrast, DL-based authentication using LSTM [73] ensures device recognition resilience against signal imperfections, albeit with limitations in severe attack detection.

Deep Neural Networks (DNNs) have integrated Intrusion Detection Systems (IDSs) to classify substantial attacks in IoT environments [74]. DNN's performance validation involved cross-validations, subsampling, and parameter optimization through grid search. Effective across various datasets, DNN excels even with imbalanced and distorted results.

DL techniques extend to safeguarding Social IoT (SIoT) [75], where DL methods propagate through fog nodes, enabling distributed threat identification. SIoT-focused DL solutions demonstrate superior attack detection capabilities, surpassing other machine learning strategies.

In network attack identification, deep Eigen space learning [76] targeted dense random networks, effectively detecting IoT gateway attacks. However, optimal parameter settings are essential for accurate classification.

IoT healthcare environments employed layering-based deep Q-networks, safeguarding protection, privacy, access control, and authentication. Deep Q-networks identified medical data based on packet features, achieving heightened accuracy through optimal feature extraction.

The Internet of Battlefield Things (IoBT) employed a deep Eigen space learning approach for malware detection [39], classifying malware using OpCode device sequences. While effective, the technique demands substantial computation, limiting its scalability to extensive datasets.

IoT-specific network features, including tiny endpoints and daily packet cycles, were employed for Distributed Denial of Service (DDoS) attack detection [68]. IoT botnet detection leveraged deep autoencoders [77], capturing N-BaIoT functions, while Bi-directional LSTM-RNN (BLSTM-RNN) [78] and autoencoders employed text identification and deep learning for IoT botnet detection, respectively.

In Industrial IoT (IIoT), deep autoencoders and deep feedforward neural networks [78] secured networks against various threats. Further research is needed to optimize intrusion mitigation protocols in IIoT.

DL techniques extend beyond individual systems to distributed environments, demonstrating superior cyberattack identification capabilities. Distributed detection architectures outperformed centralized counterparts, showcasing enhanced accuracy, lower false alarm rates, and efficient planning against cyber threats. Research avenues include comparative assessments across distributed DL and traditional learning methods on diverse datasets, as well as deeper exploration of network load data analysis for intrusion detection.

7. Solutions to IoT Threat Using DL

A security program encompasses a set of protocols and guidelines meticulously crafted to shield an organization's vital data and valuable assets. While focusing on statistical insights and other pertinent information, it diverges from delving into individuals' personal particulars. In contrast, privacy programs center their efforts on safeguarding sensitive data such as passwords, login credentials, and other confidential information. The foundation of security rests upon three fundamental pillars: upholding privacy, preserving the integrity of data and information, and ensuring unfettered accessibility.

At the core of privacy lies the fundamental right to safeguard one's personal and organizational data from unwarranted exposure. Security measures contribute to the preservation of this confidentiality, underscored by the pivotal importance of maintaining the secrecy of credentials and controlling access to critical information. These intertwined aspects form the bedrock of a resilient and comprehensive security framework.

7.1 Security Solution

Based on the research conducted by Diro and Chilamkurti [33], fog computing has shown promise in reducing the risk of eavesdropping and mitigating Man-in-the-Middle (MiTM) attacks. This is achieved by constraining communication interactions to IoT devices situated in close proximity, particularly during flooding attacks.

The research by Diro and Chilamkurti [33] illustrates how fog computing can effectively mitigate the risk of both espionage in communications and Man-in-the-Middle (MiTM) attacks. This is accomplished by confining interactions to IoT devices in close proximity, particularly during flooding attacks. Building on this concept, they put their approach into practice by utilizing the long short-term memory (LSTM) method, known for its ability to capture historical data. To assess their findings against a benchmark, they employed the ISCX2012 dataset, encompassing 71,617 instances of DoS attacks and 440,991 instances of normal traffic.

Despite LSTM model training demanding more time compared to the LR model, it demonstrated a notable 9% increase in accuracy. Subsequently, another study [80] extended these techniques to the Aegean Wi-Fi Intrusion Dataset (AWID), which included diverse instances like normal traffic, injection attacks, impersonation attacks, and flooding attacks. LSTM excelled in multiclass classification, surpassing softmax with a remarkable 14% accuracy improvement.

Further reinforcing this trend, Abeshu et al. [32] identified IoT devices' susceptibility to Denial of Service (DoS) attacks due to their limited resources. In the context of the expansive IoT network, traditional machine learning techniques prove less scalable and accurate in cyberattack detection. Leveraging the vast data generated by billions of IoT devices, deep learning models exhibit superior performance compared to shallow algorithms in the realm of learning and detection.

The authors of [32] emphasized that many deep learning architectures they used incorporated pretraining for feature extraction, streamlining abnormality detection and reducing the workload for network administrators. Their focus, however, revolved around networked deep learning involving model and parameter exchange tailored for fog computing applications. Fog computing, by alleviating the processing and storage burden on IoT

devices, becomes an ideal environment for intrusion detection. In the context of fog-to-things-based computing, traditional stochastic gradient descent (SGD) algorithms necessitate parallel computing, as the vast influx of IoT-generated data can overwhelm centralized SGD.

To address this, the study introduced a distributed deep learning-driven Intrusion Detection System (IDS) utilizing a dataset like NSL-KDD. Stacked autoencoder (SAE) was deployed for feature extraction, while softmax regression (SMR) handled data classification. SAE demonstrated superior performance in deep learning compared to existing shallow algorithms in terms of accuracy, FAR, and DR. The claims made by the authors in [60, 61] regarding the superior performance of deep learning models over shallow machine learning algorithms find support in this study.

In another work by Tan et al. [63], an attempt was made to detect Denial of Service (DoS) using a triangle-area-based technique within multivariate correlation analysis (MCA). The method involved creating features from data reaching the target network, minimizing overhead. Geometrical connections between distinct characteristics were identified using the "triangle area map" module to enhance zero-day attack detection accuracy. Earth Mover's Distance (EMD) was applied to measure deviations from observed traffic against a prebuilt normal profile. This approach was further evaluated using the KDDCup99 and ISCX datasets, achieving sample-wise correlations of 99.95% and 90.12%, respectively. However, the research did not address the impact of data size on various sample sizes, and the non-linearity of the expected change challenged the practicality of MCA.

In the context of the Internet of Things (IoT), botnet attacks represent a distinctive form of DoS attack. Authors in [69] developed an IDS that integrated Artificial Neural Networks (ANN), Decision Trees (DT), and Naive Bayes (NB) to combat botnet attacks targeting DNS, MQTT, and HTTP protocols. The ensemble approach outperformed individual algorithms in the ensemble, achieving 99.54% accuracy on the UNSW dataset and 98.29% on the NIMS dataset. MiTM attacks, closely related to DoS attacks, are among the most prevalent threats in IoT networks.

Various technological solutions have been proposed for different IoT application scenarios, driven by the limitations of traditional feedforward neural networks in handling time-series and sequence data due to their causal structure. For instance, the work of [42] showcased how LSTM-RNN thwarted an impersonation attack on smart healthcare systems, addressing the vanishing gradient issue and enhancing accuracy. Wang et al. [44] leveraged physical unclonable function (PUF) for RF communication authentication, achieving device identification and training despite initial device offsets. Aonzo et al. [43] employed deep feature selection and extraction using SAE, C4.5, ANN, and SVM, attaining 99.92% accuracy in combating impersonation attacks.

In the context of Android malware detection, Azmoodeh et al. [39] differentiated between safe and malicious software using OpCode-based deep convolutional networks, yielding 99.68% accuracy. Aonzo et al. [72] adopted static analysis, achieving 98.9% accuracy by developing new characteristics guided by commonly used qualities. Wei et al. [40] employed dynamic analysis and KNN to achieve 90% accuracy.

Machine learning (ML) has been extensively utilized for intrusion detection systems (IDSs) in IoT. Javaid et al. [79] employed STL with SAE and SMR, while Ambusaidi et al. [81] utilized mutual information for multiclass classification. Fernandez Maimo et al. [172] focused on anomaly detection using LSTM, reducing features with DBN and SAE models. DFEL was proposed in [82], outperforming conventional methods in terms of recall and runtime.

Introducing fog computing to IoT IDSs, [83] created a distributed solution that excelled in accuracy, FRP, and TPR compared to NB, ANN, and conventional ELM approaches. While fog computing demonstrated quicker attack detection than cloud-based alternatives, the study lacked a comparative analysis of current ML/DL-based fog computing algorithms. These endeavors collectively underline the growing potential of ML and DL in addressing IoT security challenges.

7.2 Privacy Solution

Numerous studies have leveraged ML to defend against MiTM threats, employing a PHY-layer authentication scheme based on Impersonation Attack Graph (IAG) that enhances detection accuracy while reducing

communication overhead. Researchers improved False Acceptance Rate (FAR), Detection Rate (DR), and computing costs by updating the dataset. Wearable device issues and user authentication complexities were highlighted, emphasizing the need for device authentication itself. While wearable devices could authenticate users, unnoticed failures could grant attackers unrestricted system access.

To enhance security, robust authentication via Bluetooth encryption and hardware-based fingerprinting was advocated. A proposed framework [96] employed classic protocol packet-based and inter-packet timing-based analysis for Bluetooth, achieving 98.5% accuracy by selecting the optimal algorithm from twenty training results.

In healthcare, privacy challenges arise due to data disclosure concerns. Non-linear kernel SVM [87] categorized medical data effectively, ensuring privacy for both service providers and user data models. Zhu et al. [87] achieved 94% classification accuracy while safeguarding privacy, categorizing users' private information and model outputs as model-privacy and learning-privacy issues. A uniform oblivious evaluation of a multivariate polynomial algorithm [85] highlighted model privacy, demonstrating safety against intrusions.

Addressing student privacy, Ma et al. [86] explored public key encryption for user data in the cloud. A cloud service provider delivered encrypted client data to a data training system, preserving privacy without revealing training specifics. Privacy-preserving DL multiple-keys (PDLM) [86] maintained privacy while applying hyperplane decision-based private methods.

Social media platforms also raise privacy concerns. While machine learning algorithms successfully thwart attacks, their slow learning pace hampers real-time efficiency. A multistage detection framework [84] combined deep learning with mobile terminal and cloud server computations, achieving around 91% accuracy using the Sino Weibo dataset and CNN. Researchers deployed distributed ML methods, collaborative Intrusion Detection Systems (IDS), and dynamic differential privacy to safeguard training datasets.

8. New Insights in Machine and Deep Learning for IoT Security

Commonly, commercial IoT devices lack robust software solutions, leaving them vulnerable. With diverse IoT use cases, software-level security is inadequate [21], raising privacy and security concerns.

Data privacy poses a significant challenge to IoT security, as highlighted by extensive research [27, 50]. Vulnerabilities like unauthorized access, eavesdropping, data manipulation, and unlawful remote entry through devices are evident [88]. For instance, personal data stored in the cloud, including names, addresses, and financial details, remains at risk. Numerous IoT devices and apps grant access to critical information, inviting attackers to exploit system vulnerabilities. Consequently, unprotected and unencrypted sensitive data may be exposed to unauthorized parties.

8.1 *IoT Vulnerabilities:* The IoT landscape is riddled with susceptibilities, stemming from its sensitive nature [181]. The intricate IoT ecosystem amplifies security risks, particularly in cloud-based systems [89]. Centralized management and legacy systems pose grave threats, while user-generated weaknesses at the application layer can arise. Notably, distinct vulnerabilities are observed:

- *Weak Passwords:* Easily guessed or hardcoded credentials jeopardize systems [27], necessitating robust, changeable passwords.
- *Insufficient Privacy Protection:* Mishandling user data within IoT ecosystems risks security flaws, demanding stringent privacy measures.
- *Exploitable Interfaces:* External interfaces like APIs and cloud services can be exploited, demanding strong authentication, encryption, and input filtering [303–310].
- *Lack of Hardening:* Absence of hardening measures allows attackers to extract critical information for remote attacks, underscoring the need for default password modification and stringent security measures .

9. Authorization, Authentication, and Identification.

IoT devices grapple with myriad security challenges, notably the incapability to achieve distinctive identification, verification, and network access. The pivotal realms of IoT device authorization, authentication, and identification raise significant apprehensions among researchers [6]. Many IoT devices lack the ability to singularly achieve identification, authentication, and authorization, leading to heightened complexities.

Furthermore, authentication poses a notable hurdle. Implementing access control mechanisms is imperative to thwart unauthorized users from exploiting network resources. A survey by authors in [90] highlighted the scarcity of protocols ensuring user safety and confidentiality among IoT communication protocols. Consequently, a pressing need persists for further research to enhance a framework that bolsters privacy and security for IoT device users, addressing the essential imperatives of IoT fortification.

10. Challenges, Limitations, and Future Directions

Recent advancements in machine and deep learning algorithms have excluded cryptographic applications from their scope. Studies [59] illustrate the potential misuse of ML, revealing SVM-based attacks on cryptographic systems. Similarly, [59] demonstrated DL's ability to decode cryptographic frameworks. CNN and AE algorithms outperformed SVM, RF, and logical process profiling methods. RNNs displayed aptitude in decryption learning. Successful internal representations were employed to decode the enigma machine through a 3000-unit LSTM-powered RNN. These findings hint at RNN's ability to manage polyalphabetic ciphers. This ML/DL research holds promise for bolstering IoT evolution. Given IoT's vast intelligent device network, robust authentication protocols for endpoints (profiles, trust connections, timestamps, privileges, encryption) are pivotal [14].

11. The limitations of Deep Learning (DL)

Our comprehensive review underscores the need for a transformative shift in existing research to meet elevated security demands within IoT settings. Security concerns, encompassing authorization, entry security, system security, data integrity, intrusion detection techniques, and packet analysis, hold paramount importance in anomaly detection. The gravity of security issues is substantial. Notably, specific factors like the chosen Intrusion Detection System (IDS) algorithm, data preprocessing, function extraction, and the optimal feature set significantly influence DL-based anomaly detection. Common challenges within deep learning methodologies pertain to flexibility and strategic planning. In [21], researchers explored diverse Deep Neural Network (DNN) models, revealing that incremental precision enhancements require extended durations. Parameter tuning is equally noteworthy, as the number of layers and accuracy exhibit a linear relationship, entailing numerous hyperparameters. This becomes particularly pertinent for deep learning methods highly responsive to data structure and size. Key research challenges in the domain of DL-based IoT security encompass: (i) Comprehensive end-to-end security (integrity, access management, authentication, confidentiality, and intrusion detection systems). (ii) Addressing intricacies in data preprocessing, optimal function selection, and extraction techniques.

12. Future Directions of DL.

Developing contemporary IoT network architectures, fortified with protective protocols encompassing authentication, access control, confidentiality, and sophisticated intrusion detection, stands as a potent remedy for comprehensive end-to-end security. Novel IoT designs must prioritize quality of service, favoring it over mere efficiency, while seamlessly integrating emerging paradigms like Software-Defined Networking (SDN) and the potential of fog-enabled IoT. The deployment of optimization algorithms, ranging from Genetic Algorithms (GAs) and Bacterial Foraging Optimization (BFO) to Particle Swarm Optimization (PSO) and attribute extraction, complemented by parameter refinement, can elevate system performance. The augmentation of efficiency without substantial computational overhead can be achieved through the application of hybrid deep learning techniques. Moreover, harnessing Blockchain technology, underpinned by deep learning, holds promise in enhancing IoT stability. By leveraging Blockchain's innate capabilities, a relatively nascent yet powerful solution emerges for ensuring the confidentiality and security of distributed records.

Conclusion

The intricacies of IoT networks lead to numerous challenges in traditional security and privacy approaches. However, leveraging Deep Learning (DL) and Machine Learning (ML) can align IoT devices more effectively with real-life scenarios. This review encompasses a range of IoT threats, exploring DL and ML as avenues for multiple potential security solutions. Various DL and ML models are exemplified, demonstrating their practicality in IoT security. State-of-the-art approaches for IoT privacy and security, driven by the integration of deep learning and machine learning techniques, are detailed. The study not only delves into machine learning's privacy and security concerns but also synthesizes a review of IoT threats by drawing on prior DL and ML studies. Novel insights into the application of ML and DL in IoT security are provided, alongside considerations of future directions, security challenges, limitations, and recommendations, all geared towards empowering forthcoming technology.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: a survey on enabling technologies, protocols, and applications," *IEEE communications surveys & tutorials*, vol. 17, no. 4, pp. 1337–1366, 2015.

[2] A. Sharma, P. K. Singh, and Y. Kumar, "An integrated fire detection system using IoT and image processing technique for smart cities," *Sustainable Cities and Society*, vol. 61, Article ID 101322, 2020.

[3] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, 2020.

[4] F. Hussain, *Internet of 1ings: Building Blocks and Business Models*, Springer, New York, NY, USA, 2017.

[5] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of 1ings Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[6] M. Abomhara and G. M. K�ien, "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks," *Journal of Cyber Security and Mobility*, vol. 4, no. 1, pp. 65–88, 2015. Security and Communication Networks

[7] S. Ray, Y. Jin, and A. Raychowdhury, ")e changing computing paradigm with internet of things: a tutorial introduction," *IEEE Design & Test*, vol. 33, no. 2, pp. 76–96, 2016.

[8] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[9] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "Corrauc: A Malicious Bot-Iot Traffic Detection Method in Iot Network Using Machine Learning Techniques," *IEEE Internet of 1ings Journal*, vol. 8, 2020.

[10] H. Li, K. Ota, and M. Dong, "Learning IoT in edge: deep learning for the internet of things with edge computing," *IEEE network*, vol. 32, no. 1, pp. 96–101, 2018.

[11] E. Fernandes, A. Rahmati, K. Eykholt, and A. Prakash, "Internet of things security research: a rehash of old ideas or new intellectual challenges?" *IEEE Security & Privacy*, vol. 15, no. 4, pp. 79–84, 2017.

[12] A. E. Omolara, A. Alabdulatif, O. I. Abiodun et al., ", internet of things security: a survey ncompassing unexplored areas and new insights," *Computers & Security*, vol. 112, Article ID 101484, 2022.

[13] S. Yao, Y. Zhao, A. Zhang et al., "Deep learning for the internet of things," *Computer*, vol. 51, no. 5, pp. 32–41, 2018.

[14] A. Riahi Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of)ings," *Digital Communications and Networks*, vol. 4, no. 2, pp. 118–137, 2018.

[15] P. Podder, M. R. H. Mondal, S. Bharati, and P. K. Paul, "Review on the security threats of internet of things," *International Journal of Computer Application*, vol. 176, no. 41, pp. 37–45, 2020.

[16] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of)ings," *Journal of Network and Computer Applications*, vol. 84, pp. 5–37, 2017.

[17] I. Yaqoob, E. Ahmed, M. H. Rehman et al., "The rise of ransomware and emerging security challenges in the Internet of Things," *Computer Networks*, vol. 129, pp. 444–458, 2017.

[18] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications surveys & tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.

[19] P. Mishra, V. Varadharajan, U. Tupakula, and E. S. Pilli, "A detailed investigation and analysis of using machine learning techniques for intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 686–728, 2019.

[20] Y. Otoum and A. Nayak, "On Securing IoT from Deep Learning Perspective," in *roceedings of the 2020 IEEE Symposium on Computers and Communications (ISCC)*, Rennes, France, July 2020.

[21] W. Liu, Z. Wang, X. Liu, N. Zeng, Y. Liu, and F. E. Alsaadi, "A survey of deep neural network architectures and their applications," *Neurocomputing*, vol. 133, pp. 11–26, 2017.

[22] M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, I. Ali, and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," *IEEE Communications Surveys & Tutorials*, vol. 22, 2020.

[23] S. Zhang, L. Yao, A. Sun, and Y. Tay, "Deep learning based recommender system: a survey and new perspectives," *ACM Computing Surveys*, vol. 52, no. 1, pp. 1–38, 2020.

[24] P. V. Klaine, M. A. Imran, O. Onireti, and R. D. Souza, "A survey of machine learning techniques applied to self-organizing cellular networks," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 1382–1421, 2017.

[25] K. Ota, M. S. Dao, V. Mezaris, and F. G. B. D. Natale, "Deep learning for mobile multimedia: a survey," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 13, no. 3s, pp. 1–22, 2017.

[26] M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, "Deep learning for IoT big data and streaming analytics: a survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2923–2960, 2018.

[27] F. Hussain, S. A. Hassan, R. Hussain, and E. Hossain, "Machine learning for resource management in cellular and IoT networks: potentials, current solutions, and open challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1150–1275, 2020.

[28] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of threats to the internet of things," *IEEE communications surveys & tutorials*, vol. 21, no. 2, pp. 1636–1675, 2019.

[29] I. Butun, P. Osterberg, and H. Song, "Security of the internet of things: vulnerabilities, attacks, and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 616–644, 2020.

[30] F. Restuccia, S. D'Oro, and T. Melodia, "Securing the internet of things in the age of machine learning and softwaredefined networking," *IEEE Internet of 1ings Journal*, vol. 5, no. 6, pp. 4829–4842, 2018.

[31] M. Al-Rubaie and J. M. Chang, "Privacy-preserving machine learning: threats and solutions," *IEEE Security & Privacy*, vol. 17, no. 2, pp. 49–58, 2019.

[32] A. Abeshu and N. Chilamkurti, "Deep learning: the Frontier for distributed attack detection in fog-to-things computing," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 169–175, 2018.

[33] A. Diro and N. Chilamkurti, "Leveraging LSTM networks for attack detection in fog-to-things communications," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 124–130, 2018.

[34] Z. Tan, A. Jamdagni, X. He, P. Nanda, R. P. Liu, and J. Hu, "Detection of denial-of-service attacks based on computer vision techniques," *IEEE Transactions on Computers*, vol. 64, no. 9, pp. 1509–1523, 2015.

[35] C. Tselios, I. Politis, and S. Kotsopoulos, "Enhancing SDN Security for IoT-Related Deployments through Blockchain," in *Proceedings of the 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, pp. 303–308, IEEE, Forum, Berlin, November 2017.

[36] X. Jing, Z. Yan, X. Jiang, and W. Pedrycz, "Network traffic fusion and analysis against DDoS flooding attacks with a novel reversible sketch," *Information Fusion*, vol. 51, pp. 100–113, 2019.

[37] M. Rezazad, M. R. Brust, M. Akbari, P. Bouvry, and N.-M. Cheung, "Detecting Target-Area Link-Flooding Ddos Attacks Using Traffic Analysis and Supervised Learning," *Advances in Intelligent Systems and Computing*, Springer, New York, NY, USA, 2018.

[38] N. Moustafa, B. Turnbull, and K.-K. R. Choo, "An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things," *IEEE Internet of 1ings Journal*, vol. 6, no. 3, pp. 4815–4830, 2019

[39] A. Azmoodeh, A. Dehghantanha, and K.-K. R. Choo, "Robust malware detection for internet of (battlefield) things devices using deep eigenspace learning," *IEEE Transactions on Sustainable Computing*, vol. 4, no. 1, pp. 88–95, 2019.

[40] L. Wei, W. Luo, J. Weng, Y. Zhong, X. Zhang, and Z. Yan, "Machine learning-based malicious application detection of android," *IEEE Access*, vol. 5, Article ID 15491, 2017.

[41] S. Sharmeen, S. Huda, J. H. Abawajy, W. N. Ismail, and M. M. Hassan, "Malware threats and detection for industrial mobile-IoT networks," *IEEE Access*, vol. 6, Article ID 15941,2018.

[42] U. Ahmad, H. Song, A. Bilal, S. Saleem, and A. Ullah, "Securing Insulin Pump System Using Deep Learning and Gesture Recognition," in *Proceedings of the 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, New York, NY, USA, August 2018.

[43] M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo, and K. Kim, "Deep abstraction and weighted feature selection for Wi-Fi impersonation detection," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 3, pp. 621–636, 2018.

[44] B. Chatterjee, D. Das, and S. Sen, "RF-PUF: IoT Security Enhancement through Authentication of Wireless Nodes Using In-Situ Machine Learning," in *Proceedings of the 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 103–106, IEEE, Washington,DC, USA, April 2018.

[45] N. Wang, T. Jiang, S. Lv, and L. Xiao, "Physical-layer authentication based on extreme learning machine," *IEEE Communications Letters*, vol. 21, no. 7, pp. 1557–1560, 2017.

[46] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of things (IoT): taxonomy of security attacks," in *Proceedings of the 2016 3rd International Conference on Electronic Design (ICED)*, pp. 321–326, IEEE, Phuket,)ailand, 2016.

[47] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: challenges," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 26–33, 2017.

[48] A. C. Jose and R. Malekian, "Improving smart home security: integrating logical sensing into smart home," *IEEE Sensors Journal*, vol. 17, no. 13, pp. 4168–4286, 2017.

[49] A. Gharaibeh, M. A. Salahuddin, S. J. Hussini et al., "Smart cities: a survey on data management, security, and enabling technologies," *IEEE Commun. Surveys Tuts.*vol. 19, no. 4, pp. 1446–1491, 2017.

[50] D. Eckhoff and I. Wagner, "Privacy in the smart city—applications, technologies, challenges, and solutions," *IEEE Commun. Surveys Tuts.*vol. 20, no. 1, pp. 489–516, 2018.

[51] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for internet of things: a survey," *IEEE Internet of 1ings Journal*, vol. 3, no. 1, pp. 70–95, Feb. 2016.

[52] A. Stanciu, T.-C. Balan, C. Gerigan, and S. Zamfir, "Securing the IoT gateway based on the hardware implementation of a multi pattern search algorithm," in *Proceedings of the 2017*

[53] H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub, "'A comprehensive IoT attacks survey based on a buildingblocked reference model," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 3, pp. 355–373, 2018.

[54] S. Shadroo, A. M. Rahmani, and A. Rezaee, "The two-phase scheduling based on deep learning in the Internet of Things," *Computer Networks*, vol. 185, Article ID 107684, 2021.

[55] F. Liang, W. Yu, X. Liu, D. Griffith, and N. Golmie, "Toward edge-based deep learning in industrial Internet of Things," *IEEE Internet of 1ings Journal*, vol. 7, no. 5, pp. 4329–4341, 2020.

[56] Z. M. Fadlullah, F. Tang, B. Mao et al., "State-of-the-art deep learning: evolving machine intelligence toward tomorrow's intelligent network traffic control systems," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 1422–1445, 2017.

[57] I. Goodfellow, Y. Bengio, A. Courville, and Y. Bengio, *Deep Learning*, MIT press, Cambridge, MA, USA, 2016.

[58] E. De Coninck, V. Tim, V. Bert et al., "Distributed Neural Networks for Internet of Things:)e Big-Little Approach," *Internet of 1ings. IoT Infrastructures. IoT360 2015*, pp. 484–492, Springer, New York, NY, USA, 2015.

[59] H. Maghrebi, T. Portigliatti, and E. Prouff, "Breaking Cryptographic Implementations Using Deep Learning Techniques," *Security, Privacy, and Applied Cryptography Engineering. SPACE 2016*, pp. 3–26, Springer, New York, NY, USA, 2016.

[60] R. Pascanu, C. Gulcehre, K. Cho, and Y. Bengio, "How to construct deep recurrent neural networks," 2013, https://arxiv. org/abs/1312.6026#::text﷿By%20carefully%20analyzing% 20and%20understanding,hidden% 2Dto%2Doutput%20function.

[61] M. Hermans and B. Schrauwen, "Training and analysing deep recurrent neural networks," *Advances in Neural Information Processing Systems*, vol. 26, pp. 190–198, 2013.

[62] H. F. Nweke, Y. W. Teh, M. A. Al-Garadi, and U. R. Alo, "Deep learning algorithms for human activity recognition using mobile and wearable sensor networks: state of the art and research challenges," *Expert Systems with Applications*, vol. 105, pp. 132–160, 2018.

[63] P. Torres, C. Catania, S. Garcia, and C. G. Garino, "An Analysis of Recurrent Neural Networks for Botnet Detection Behavior," in *Proceedings of the 2016 IEEE Biennial Congress of Argentina (ARGENCON)*, pp. 1–6, IEEE, Buenos Aires, Argentina, 2016.

[64] U. Fiore, F. Palmieri, A. Castiglione, and A. De Santis, "Network anomaly detection with the restricted Boltzmann machine," *Neurocomputing*, vol. 122, pp. 13–23, 2013.

[65] Y. Chen, Y. Zhang, S. Maharjan, M. Alam, and T. Wu, "Deep learning for secure mobile edge computing in cyber-physical transportation systems," *IEEE Network*, vol. 33, no. 4, pp. 36–41, 2019.

[66] M. Yousefi-Azar, V. Varadharajan, L. Hamey, and U. Tupakula, "Autoencoder-based Feature Learning for Cyber Security Applications," in *Proceedings of the 2017 International Joint Conference on Neural Networks (IJCNN)*, pp. 3854–3861, IEEE, Anchorage, AK, USA, 2017.

[67] I. Goodfellow, J. Pouget-Abadie, M. Mehdi et al., "Generative adversarial nets," in *Proceedings of the 27th International Conference on Neural Information Processing Systems - Volume 2*, Montreal, Canada, 2014.

[68] R. E. Hiromoto, M. Haney, and A. Vakanski, "A secure architecture for IoT with supply chain risk management,"vol. 1, pp. 431–435, in *Proceedings of the 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, vol. 1, IEEE, Bucharest, Romania, 2017.

[69] N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, and R. Salakhutdinov, "Dropout: a simple way to prevent neural networks from overfitting," *Journal of Machine Learning Research*, vol. 15, no. 1, pp. 1929–1958, 2014.

[70] G. Huang, Y. Sun, Z. Liu, D. Sedra, and K. Q. Weinberger, "Deep networks with stochastic depth," in *European Conference on Computer Vision*, Springer, New York, NY, USA, 2016.

[71] T. T. Nguyen and V. J. Reddi, "Deep Reinforcement Learning for Cyber Security," 2019, tps://arxiv.org/abs/1906.05799.

[72] A. Ferdowsi and W. Saad, "Deep Learning-Based Dynamic Watermarking for Secure Signal Authentication in the Internet of)ings," in *Proceedings of the 2018 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, Kansas City, MO, USA, May 2018.

[73] R. Das, A. Gadre, S. Zhang, S. Kumar, and J. M. F. Moura, "A Deep Learning Approach to IoT Authentication," in *Proceedings of the 2018 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, Kansas City, MO, USA, May 2018.

[74] B. A. Tama and K.-H. Rhee, "Attack classification analysis of IoT network via deep learning approach," *Res. Briefs Inf. Commun. Technol. Evol.(ReBICTE)*, vol. 3, pp. 1–9, 2017.

[75] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," *Future Generation Computer Systems*, vol. 82, pp. 761–768, 2018.

[76] O. Brun, Y. Yin, E. Gelenbe, Y. M. Kadioglu, J. AugustoGonzalez, and M. Ramos, "Deep Learning with Dense Random Neural Networks for Detecting Attacks against IoT Connected home Environments," *Communications in Computer and Information Science*, Springer Cham, New York, NY, USA, 2018.

[77] Y. Meidan, M. Bohadana, Y. Mathov et al., "N-baiot—network-based detection of iot botnet attacks using deep autoencoders," *IEEE Pervasive Computing*, vol. 17, no. 3, pp. 12–22, 2018.

[78] M. Al-Hawawreh, N. Moustafa, and E. Sitnikova, "Identi-fication of malicious activities in industrial internet of things based on deep learning models," *Journal of Information Security and Applications*, vol. 41, pp. 1–11, 2018.

[79] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," *Eai Endorsed Transactions on Security and Safety*, vol. 3, no. 9, p. e2, 2016.

[80] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, "Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 184–106, 2016.

[81] M. A. Ambusaidi, X. He, P. Nanda, and Z. Tan, "Building an intrusion detection system using a filter-based feature selection algorithm," *IEEE Transactions on Computers*, vol. 65, no. 10, pp. 2986–2998, 2016.

[82] Y. Zhou, M. Han, L. Liu, J. S. He, and Y. Wang, "Deep Learning Approach for Cyberattack Detection," in *Proceedings of the IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* Honolulu, HI, USA, April 2018.

[83] S. Prabavathy, K. Sundarakantham, and S. M. Shalinie, "Design of cognitive fog computing for intrusion detection in Internet of Things," *Journal of Communications and Networks*, vol. 20, no. 3, pp. 291–298, 2018.

[84] B. Feng, Q. Fu, M. Dong, D. Guo, and Q. Li, "Multistage and elastic spam detection in mobile social networks through deep learning," *IEEE Network*, vol. 32, no. 4, pp. 15–21, 2018.

[85] Q. Jia, L. Guo, Z. Jin, and Y. Fang, "Preserving model privacy for machine learning in distributed systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 29, no. 8, pp. 1808–1822, 2018.

[86] X. Ma, J. Ma, H. Li, Q. Jiang, and S. Gao, "PDLM: PrivacyPreserving Deep Learning Model on Cloud with Multiple Keys," *IEEE Transactions on Services Computing*, vol. 14, 2018.

[87] H. Zhu, X. Liu, R. Lu, and H. Li, "Efficient and privacypreserving online medical prediagnosis framework using nonlinear SVM," *IEEE journal of biomedical and health informatics*, vol. 21, no. 3, pp. 838–850, 2017.

[88] A. E. Omolara, A. Jantan, O. Isaac Abiodun, K. Victoria Dada, H. Arshad, and E. Emmanuel, "A deception model robust to eavesdropping over communication for social network systems," *IEEE Access*, vol. 7, Article ID 100881, 2019.

[89] N. Torres, P. Pinto, and S. I. Lopes, "Security vulnerabilities in LPWANs—an attack vector analysis for the IoT ecosystem," *Applied Sciences*, vol. 11, no. 7, p. 3176, 2021.

[90] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of)ings," *Ad Hoc Networks*, vol. 32, pp. 17–31, 2015.

[91] Q. Zhang and X. Wang, "SQL injections through back-end of RFID system," in *Proceedings of the 2009 International Symposium on Computer Network and Multimedia Technology*, pp. 1–4, Wuhan, China, January 2009.

[92] S. Tofigh, M. O. Ahmad, and M. N. S. Swamy, "A low complexity modified)iNet algorithm for pruning convolutional neural networks," *IEEE Signal Processing Letters*, vol. 29, pp. 1012–1016, 2022.

[93] D. Scherer, A. M¨uller, and S. Behnke, "Evaluation of Pooling Operations in Convolutional Architectures for Object Recognition," *Artificial Neural Networks – ICANN 2010*, pp. 92–101, Springer, Berlin, Germany, 2010.

[94] A. Graves, A.-r. Mohamed, and G. Hinton, "Speech Recognition with Deep Recurrent Neural Networks," in *Proceedings of the 2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 6645–6649, IEEE, Vancouver, BC, Canada, May 2013.

[95] I. Goodfellow, J. Pouget-Abadie, M. Mehdi et al., "Generative adversarial nets," in *Proceedings of the 27th International Conference on Neural Information Processing Systems - Volume 2*, Montreal, Canada, 2014.

[96] H. Aksu, A. S. Uluagac, and E. Bentley, "Identification of Wearable Devices with Bluetooth," *IEEE Transactions on Sustainable Computing*, vol. 6, 2018.