Machine Learning-Enabled IoT Security: Open Issues and Challenges Under Advanced Persistent Threats

ZHIIYAN CHEN, JINXIN LIU, YU SHEN, MURAT SIMSEK, BURAK KANTARCI, and HUSSEIN T. MOUFTAH, University of Ottawa
PETAR DJUKIC, Ciena

Despite its technological benefits, the Internet of Things (IoT) has cyber weaknesses due to vulnerabilities in the wireless medium. Machine Learning (ML)-based methods are widely used against cyber threats in IoT networks with promising performance. An Advanced Persistent Threat (APT) is prominent for cybercriminals to compromise networks, and it is crucial to long-term and harmful characteristics. However, it is difficult to apply ML-based approaches to identify APT attacks to obtain a promising detection performance due to an extremely small percentage among normal traffic. There are limited surveys that fully investigate APT attacks in IoT networks due to the lack of public datasets with all types of APT attacks. It is worth bringing the state of the art in network attack detection with APT attack detection in a comprehensive review article. This survey article reviews the security challenges in IoT networks and presents well-known attacks, APT attacks, and threat models in IoT systems. Meanwhile, signature-based, anomaly-based, and hybrid intrusion detection systems are summarized for IoT networks. The article highlights statistical insights regarding frequently applied ML-based methods against network intrusion. Finally, open issues and challenges for common network intrusion and APT attacks are presented for future research.

CCS Concepts: • Security and privacy → Intrusion detection systems; Network security; • Computing methodologies → Machine learning; • Networks → Sensor networks;

Additional Key Words and Phrases: Internet of Things, cyberattack, network security, network intrusion detection, machine learning, deep learning

ACM Reference format:
Zhiyan Chen, Jinxin Liu, Yu Shen, Murat Simsek, Burak Kantarci, Hussein T. Mouftah, and Petar Djukic. 2022. Machine Learning-Enabled IoT Security: Open Issues and Challenges Under Advanced Persistent Threats. ACM Comput. Surv. 55, 5, Article 105 (December 2022), 37 pages.
https://doi.org/10.1145/3530812

1 INTRODUCTION

The Internet of Things (IoT) is a network of devices equipped with sensing, communicating, and unique identifiable characteristics [73]. The widespread adoption of connected services that utilize IoT devices and networks has enabled IoT applications’ advancement. IoT networks offer...
smarter environments and services than earlier networks by leveraging and integrating sensed data from various sensors [73]. Embedded sensors in IoT devices communicate with peer nodes through wireless networks such as the standards developed by the 3rd Generation Partnership Project (3GPP), IEEE 802.11ah, Bluetooth Low Energy, and Z-Wave protocols [9]. Additional benefits include transparency and ease of access to information while reducing human interventions.

Due to several advantages with regard to IoT, such as improved customer engagement, reduction of waste, enhanced data collection, and technology optimization, IoT technology is being integrated into various systems (e.g., Industrial Control Systems (ICSs), modern vehicles, and Critical Infrastructure (CI)) [133]. For instance, the integration of IoT systems with CIs such as facilities, power distribution networks, and critical assets is emergent [23]. One such example is the use of IoT systems to monitor and manage CIs in the smart city context [157]. Such networks’ objective is to improve efficiency in management, production, and services of a city to make the city more livable.

Another set of IoT use cases is in industrial settings. The Industrial Internet of Things (IIoT) is a subset of IoT, which is the application of IoT applied to industrial processes by facilitating the interconnection of entities such as controllers, sensors, and actuators in industrial production and automation context [177]. IIoT is utilized in CIs that provide many essential services in the industrial setting [103]. IIoT contains closely related IoT concepts, including the same main characteristics: availability, intelligent control, and connected devices. Therefore, IoT and IIoT share some common concepts, including data management connectivity, data security, and secure cloud. However, IIoT is generally used to control and monitor industrial processes such as continuous manufacturing, supply chain monitoring, and management systems. IIoT also uses more sensitive and precise sensors, including more location-aware technologies than IoT [148].

This survey focuses on network attacks in both broad applications of IoT systems. Both general IoT and IIoT systems are vulnerable to a variety of cyberattacks. In the case of ICSs, safety is as critical as the notion of security. Safety addresses concerns such as ensuring the protection of humans, the environment, and equipment against consequences of system failures [186]. To understand the importance of some critical industrial infrastructure, think of a nuclear plan using IIoT and the consequences of a cyberattack on this infrastructure. An attack could have consequences on the personnel at the plant, and it could have broad-ranging effects on the world.

As an example, we use the architecture of a Cyber-Physical Production System (CPPS) (Figure 1), which may be a part of an IIoT-based smart factory. The architecture consists of several layers [133]. The system’s base is the actual production process—the factory consisting of the physical and production components. The IIoT system is built on top and consists of electronics,
networking, and software. Finally, humans and machines monitor the system to ensure that it is working correctly.

This IIoT system is vulnerable across multiple layers. For instance, physical layers are susceptible through invasive hardware attacks [174] and side-channel attacks. Meanwhile, social attacks (e.g., phishing attacks) arise when people operate a CPPS.

Since IoT-based systems operate on wireless channels that broadcast data, they are potentially exposed to malicious users and cybercrimes [186]. Considering the physical medium, software, and protocols, vulnerabilities combined with adversaries' competency can produce sophisticated network-based attacks on IoT systems [93].

Hackers have various motives for attacking an IoT system, including exposing, altering, disable, destroying, stealing, or gaining unauthorized access to or making unauthorized use of an asset [115]. An example is a Denial-of-Service (DoS), in which an attacker floods messages to victims by sending a large number of packets from a legitimate host network [135]. Alternatively, port scanning attacks [79] involve an attacker that detects an open port where attacks can be injected. Consequently, attackers can obtain network-related detailed information including but not limited to IP and MAC addresses. By the end of 2021, more than 10 billion IoT devices were employed in smart city and industrial management on a global scale. This number will approach 75 billion by the end of 2025 according to the study by Razzaq et al. [129]. Due to the enormous expansion of IoT devices in recent years and the vulnerability of IoT sensors, governments and businesses invest on IoT security to prevent hackers from infiltrating systems, and the investments to keep IoT devices secure remains insufficient to prevent hackers from causing economic losses of more than $1 trillion [124]. These figures demonstrate the critical significance of IoT security and its pervasive impact on daily life and economic activity.

Detecting and mitigating network intrusion is essential to secure an IoT system. For instance, as reported in the work of Kimani et al. [78], IoT-based smart grid networks, with millions of nodes, create a large attack surface. The protection of IoT systems relates primarily to sustaining the essentials for daily needs of societies and individuals [20]. In hybrid detection systems, Machine Learning (ML)-based identification methods have been researched intensively and have been shown to operate efficiently against network intrusion detection. The state of the art today contains various ML methods, some of which exhibit competitive detection levels reaching 100% [99].

An Advanced Persistent Threat (APT) intends to bypass access control mechanisms so as to control user equipment. APT attacks are crucial for users due to their long time span until the damage is done, and they are challenging for identification in a network due to hidden characteristics [54]. APT attacks are essential parts of network datasets. For instance, NSL-KDD contains U2R and R2L classes, which belong to APT attacks [68]. Moreover, backdoor, reconnaissance, Shellcode, and worms in UNSW-NB15 are also among known APT attacks. We summarize renowned datasets and classes in Table 1, which shows datasets that include various types of APT attacks. Furthermore, no public network dataset with only APT attacks exists. It is difficult to investigate APT attacks using one dataset; hence, the literature that focuses on APT attacks is limited. Typically, APT attacks occupy an extremely lower percentage (e.g., 0.046% U2R and 0.88% U2R in NSL-KDD) to disguise their patterns. Therefore, APT attack detection performance is lower than for non-APT attacks. With this in mind, this article aims to contribute to the IoT security literature by reviewing existing research on APT attacks and presenting opportunities, challenges, and open issues for further research.

Based on the efficiency of ML-based approaches in the detection of widely investigated attack types in IoT, this work aims to review these attack models in IoT-monitored CIs and review the
Table 1. Attacks in Public Datasets

| Attack Patterns | Attack | NSL-KDD | KDD99 | UNSW-NB15 | MAWLab | CICIDS2018 | AWID |
|-----------------|--------|---------|-------|-----------|---------|------------|------|
| APT Attack Patterns | Probe | ✓ | ✓ | x | x | x | x |
|                  | R2L   | ✓ | ✓ | x | x | x | x |
|                  | U2R   | ✓ | ✓ | x | x | x | x |
|                  | Backdoors | x | x | ✓ | x | x | x |
|                  | Exploits | x | x | ✓ | x | x | x |
|                  | Reconnaissance | x | x | ✓ | x | x | x |
|                  | Shellcode | x | x | ✓ | x | x | x |
|                  | Worms | x | x | ✓ | x | x | x |
|                  | Botnet | x | x | x | x | ✓ | x |
|                  | Web attacks | x | x | x | ✓ | x | x |
|                  | Infiltration | x | x | x | ✓ | x | x |
|                  | IPV6 tunneling | x | x | x | ✓ | x | x |
|                  | NetworkScan ICMP, UDP, TCP | x | x | x | ✓ | x | x |
|                  | Port Scan | x | x | x | ✓ | x | x |
|                  | Injection | x | x | x | x | ✓ | x |
|                  | Impersonation | x | x | x | x | x | ✓ |
| Non-APT Attack Patterns | DoS | ✓ | ✓ | x | ✓ | ✓ | ✓ |
|                  | Fuzzers | x | x | ✓ | x | x | x |
|                  | Analysis | x | x | ✓ | x | x | x |
|                  | DoS | x | x | ✓ | x | x | x |
|                  | Generic | x | x | ✓ | x | x | x |
|                  | Brute force | x | x | x | ✓ | x | x |
|                  | Heartbleed | x | x | x | x | ✓ | x |
|                  | DDos | x | x | x | ✓ | x | x |
|                  | HTTP | x | x | x | x | ✓ | x |
|                  | Multi. points | x | x | x | ✓ | x | x |
|                  | Alpha | x | x | x | ✓ | x | x |
|                  | Flooding | x | x | x | x | ✓ | x |

✓ means attack in dataset; x means does not belong to dataset.

use of ML algorithms to detect those attacks. Meanwhile, it is worthy to review APT attacks for future prospective directions.

Our contributions are as follows:

- We present the architectures of IoT-monitored CIs and their security vulnerabilities.
- Reviews various Artificial Intelligence (AI)-based state-of-the-art approaches to detect and mitigate network intrusions. Out of these, 14 AI methods are shortlisted based on their frequency of application.
- Public IoT datasets are summarized for attack detection research that are barely included in current literature.
- Opportunities, open issues, and challenges against APT attacks, which exist in most current network detection datasets and typically result in low detection performance, are presented.

Recently, several surveys discussed ML approaches for network intrusion, as shown in Table 2. Although ML-based approaches have emerged, it is valuable to study the legacy methodologies to understand their benefits and limitations. Moreover, APT attacks exist in many public datasets, but they are rarely studied in surveys highlighting APT attack detection via ML. Meanwhile, an IoT-specific dataset is an essential part for IoT security research using ML algorithms. However, it is difficult and expensive to deploy IoT networks for IoT data collection. Using a public IoT-targeted dataset is a cost-effective approach to set up a project and focus on methodologies. However, there
is little literature summarizing IoT-specific information. With these motivations, this article aims to bridge these gaps, including (1) studying traditional techniques and ML-based approaches for attack detection in one article, (2) focusing on APT attack detection via ML approaches, and (3) summarizing existing public IoT datasets. In Table 2, gap analysis with respect to the existing relevant surveys is shown based on the following criteria: ML and/or Deep Learning (DL), legacy Intrusion Detection System (IDS) techniques, attack and threat models, and APT consideration. Meanwhile, abbreviations used in this work are summarized in Table 3.

The structure of this survey is shown in Figure 2, and the rest of the survey is organized into the following six sections. Section 2 presents security in IoT, including security features and specific security for IIoT (e.g., ICSs). Section 3 discusses IoT attacks by also focusing on APT attacks.

### Table 2. Comparison with Related Surveys

| Ref. | ML/ DL | Non-M Techniques | Threat Model | APT | Limitations |
|------|--------|------------------|--------------|-----|-------------|
| [51] | DL     | ×                | ×            | ×   | DL-based detection methods without ML |
| [76] | Both   | ✓                | ×            | ×   | No threat analysis specific to the IoT network attack pattern |
| [41] | Both   | ×                | ×            | ×   | No discussion of non-ML-based detecting techniques and no traditional security methods |
| [32] | Both   | ✓                | ✓            | ×   | No APT attack life cycle and attack pattern discussion |
| [60] | Both   | ×                | ×            | ×   | No network attacks categorized and old datasets (around 2010) discussed |
| [13] | Both   | ×                | ✓            | ×   | Lack analysis of IoT-related datasets |
| Our  | Both   | ✓                | ✓            | ✓   | With ML, DL, and non-ML detection schemes, and analysis impact of APT attacks in the IoT context for the first time |

### Table 3. List of Abbreviations

| 3GPP       | 3rd Generation Partnership Project | ICS       | Industrial Control System |
|------------|------------------------------------|-----------|---------------------------|
| AML        | Adversarial Machine Learning       | IDS       | Intrusion Detection System |
| APT        | Advanced Persistent Threat         | IIoT      | Industrial Internet of Things |
| CI         | Critical Infrastructure            | IoT       | Internet of Things        |
| CNN        | Convolutional Neural Network       | KNN       | K-Nearest Neighbor         |
| CPPS       | Cyber-Physical Production System   | LR        | Linear Regression          |
| DAE        | Deep Autoencoder                  | LRDoS     | Low-Rate One-Class Denial-of-Service |
| DBN        | Deep Belief Network               | LSTM      | Long Short-Term Memory    |
| DBSCAN     | Density-Based Spatial Clustering of Applications with Noise | MC | Malicious Control |
| DL         | Deep Learning                     | ML        | Machine Learning           |
| DMZ        | Demilitarized Zone                | MO        | Malicious Operation        |
| DoS        | Denial-of-Service                 | OT        | Operational Technology    |
| DP         | Data Type Probing                 | PASTA     | Process for Attack Simulation and Threat Analysis |
| DS2OS      | Distributed Smart Space Orchestration System | PLC | Programmable Logic Controller |
| DT         | Decision Tree                      | RNN       | Recurrent Neural Network   |
| FCN        | Fully Connected Network            | UML       | Unified Modeling Language  |
| HMI        | Human-Machine Interface            | WS        | Wrong Setup                |

ACM Computing Surveys, Vol. 55, No. 5, Article 105. Publication date: December 2022.
Moreover, an attack taxonomy is presented with APT attack distribution. Several threat models are reviewed, and an attack analysis is presented by using the Process for Attack Simulation and Threat Analysis (PASTA) model. In Section 4, network intrusion detection methodologies for IoT are reviewed and categorized into three groups. Section 5 presents the ML-based approaches that are applied to address network attacks. Section 6 introduces open issues, challenges, and opportunities for common network intrusion and APT using ML algorithms. Finally, Section 7 concludes and summarizes the survey.

2 SECURITY IN IOT

It is widely recognized that IoT technologies and applications are still in their infancy [42]. Several challenges restrain the development and application of IoT, including technical limitations, lack of standardization, and limited security and privacy components [85]. The acceptance and ubiquity of new IoT technologies and services largely depend on the status of data security and privacy protection, which are two challenging issues for IoT because of its deployment, mobility, and complexity [43]. The study of Mahmoud et al. [98] describes IoT in a three-layer architecture, namely perception, network, and application layers. Security challenges associated with each layer are shown in Figure 3.

2.1 Security Features of IoT

The security requirements of an IoT system vary based on its purpose. An IoT system should perform its defined functions, prevent attacks, and operate with resilience when under attack [161]. A
secure and resilient IoT system needs to satisfy confidentiality, integrity, availability, and authentication features:

- **Confidentiality** aims to protect information from being accessed by unauthorized parties. Many entities are integrated into an IoT system, and each device could reveal collected data to other nodes within the network. For instance, the study of Romdhani [132] demonstrates that IoT-based e-health systems, where confidentiality is a high requirement, are vulnerable to third-party attacks. Consequently, a set of management approaches is required to ensure data security and confidentiality [10].

- **Integrity** refers to ensuring the authenticity of a piece of information (e.g., the information is not altered and the data source is genuine). Data integrity ensures the quality of service and data security and privacy [88]. With the increasing availability of cloud computing, coupled with ever-increasing volumes of data, maintaining the data’s integrity is critical, especially for outsourced data or third-party data. Measures are taken to ensure integrity, including (1) controlling the physical environment of networked terminals and servers, (2) restricting access to data, and (3) maintaining rigorous authentication practices. For instance, Seitz et al. [140] demonstrate an authorization framework distributing processing costs between constrained IoT devices and less constrained back-end servers while keeping message exchanges with the minimum constrained devices. The study of Jiang et al. [71] introduces several authentication techniques to address data integrity issues.

- **Availability** is the ability to access data or services when and where needed [131]. The priority of IoT security is to ensure the availability and functionality of each IoT application [171]. The study of Zin et al. [188] demonstrates a concept based on probability theory for measuring the reliability and availability of the IoT devices in the network.

- **Authentication** is the process of verifying a person’s identity or device and preventing unauthorized access, and misuse of related personal information [149]. In an IoT context, it is essential to deploy an authentication process because of the nature of the IoT. Specifically, several entities (e.g., equipment, users, service providers, and processing units) participate in various services and functions. For example, smart home devices may transmit sensitive information about the user's health and preferences.

![Fig. 3. IoT security challenges in each layer [98].](image-url)
in an IoT system [180]. Liu et al. [91] introduce an access control policy for authentication based on the device’s particular role(s) in the associated IoT network.

2.2 Security in Industrial IoT

Industrial control system is a general term for a series of systems used for controlling industrial processes [178]. They are widely applied in power generation, petroleum extraction and processing, water conservancy, and other industrial fields [95]. The creation of the IoT has allowed for new opportunities in industrial development [189]. For example, various sensor networks provide the necessary supervision and decision data for an ICS, which in turn allows the ICS to control the production process more efficiently and accurately [39]. However, wireless communication and vulnerabilities in IoT expose ICS to internal security risks [18]. We now introduce the essential ICS structures and analyze their vulnerabilities.

IIoT systems are targeted by cybercriminals because the content accessible in those networks can include valuable and confidential manufacturing, as well as production data [87]. It is also vital to protect IIoT systems against attacks because such systems are often interconnected to other information and communications technologies among the manufacturing processes. Internet-enabled IoT has allowed these networks to become part of the CI for business operations, including industrial control systems, which is a general term for a variety of control systems [24]. The studies in the work of Boyle and Speed [29] present CI in Canada, which has 10 categories of CI, including those mentioned for the United States as well as others such as health, food, and water.

Enterprises protect their ICSs via firewalls, which restrict and supervise the communication between the internal and external networks, aiming to ensure the overall security of the network systems [111]. According to the location and function of firewalls, the structure of the ICS can be divided into three types (e.g., dual firewall, single firewall, and multi-firewall facilities) [7]. Firewalls that are properly configured can protect an ICS via IDSs, and manage application level privileges [7].

ICS LAN is equivalent to a **Demilitarized Zone (DMZ)** for the business LAN in a single firewall architecture. The purpose of a DMZ is to add an additional layer where an external network node can only access public resources permitted in the DMZ while the rest of the network is firewalled. Dual firewalls are the most commonly used protection structure, where two firewalls separate Internet, business LAN, and ICS LAN, as shown in Figure 4. Generally, the firewall between business LAN and the Internet is operated by IT staff, whereas the other firewall is operated by ICS staff. The dual-firewall structure offers a higher security level by denying unauthorized access from external networks than using only one firewall. Business and ICS staff jointly control the single firewall that is utilized for protecting the ICS from cyberattacks. Finally, multi-firewall infrastructures are suitable for large-scale distributed control systems. This structure is based on a dual firewall containing multiple ICS LANs connected with the business LAN. Each connection between the ICS LAN and the business LAN is equipped with a firewall. When communication is required between ICS LANs, some business LANs will be selected as intermediate paths.

3 **COMMON ATTACKS, APT ATTACKS, AND THREAT MODEL ANALYSIS IN IOT**

The literature in this area is typically driven by the availability of datasets. Various datasets have been used in many of the works examined in this article, consequently leading to different standards to classify attack types.

3.1 **Common Attacks in IIoT**

The IIoT, as a derivation of IoT, experiences similar types of cyberattacks that are vulnerable to various ranges of attack. Networks, such as IIoT, are an essential asset in a business [125].
Adversaries take advantage of cybersecurity weaknesses in IIoT to (1) obtain confidential information, (2) disrupt operations, and (3) cause damage potentially to the reputation and interests of an enterprise under attack. CI is a prominent part of enterprises and industries. For example, in 2019, a CI was attacked every 14 seconds on average [5]. Meanwhile, the work presented by Morgan [5] predicted the losses caused by cyberattacks targeting enterprises to be as high as $11.5 billion at the beginning of 2022. Addressing ICS vulnerabilities in CI will minimize the negative financial impact while creating an opportunity and need for future cybersecurity research.

Among the ICS vulnerabilities [7], the simplest one is that an attacker can directly send commands to data acquisition equipment. Since most Programmable Logic Controllers (PLCs) and data acquisition servers lack basic authentication, they generally accept any information sent to them. All of the adversaries aim to establish a connection with the device via breaking in through the firewall and then send appropriate commands to take control.

Another effective attack method for the adversaries is to export the operator’s Human-Machine Interface (HMI) directly to an external device. Off-the-shelf tools can complete this operation under Windows and UNIX environments. Finally, the adversary can use a man-in-the-middle attack in which the attacker plays the role of a middleman. If the attacker needs to know the ICS protocol, they can change data packets between the HMI and the server to both deceive the operator and take control of the ICS [46].

Next is a list of some of the attacks in the IIoT literature:
• **Zero-day attacks:** Zero-day exploits refer to the time it takes from the detection of an attack to fix the design flaws that developers have not recognized at the time of release and until the vulnerability is overcome [27]. Such attacks may occur on field devices and servers. For example, using overflowing buffers, an adversary can inject malicious executable code into running programs to take command of various industrial processes.

• **Non-prioritization of tasks:** Non-prioritization of tasks is a severe flaw in many types of real-time ICSs [22]. As an example, memory sharing among the tasks with equal priority results in serious security issues. Accessibility to create an Object Entry Point in the kernel domain is a feature of VxWorks, a proprietary real-time operating system, resulting in loopholes.

• **Database injection:** Database injection exploits the vulnerabilities in an ICS [26], which widely occur in SQL-based databases. The hackers send fake SQL commands from a web server to a database server, for example, via a supervisory control and data acquisition system, subsequently obtaining unwarranted access to both data and digitally controlled industrial processes.

• **Vulnerabilities in legacy systems:** In association with a legacy system, the ICS usually lacks sufficient user and system authorization, and data authorization verification [40], leading to attackers gaining unauthorized access to the system. When faced with a new generation of ICSs, older SCADA controllers and the associated communication protocols cannot be encrypted. Attackers can discover user names and passwords by sniffing software that allows the user to monitor (“sniff”) users’ Internet traffic in real time, capturing all of the data flowing to and from the user’s computer.

• **Default setting:** Through enumeration methods, an attacker can easily crack unsafe devices with default passwords and settings [6], then control the ICS and implement a corresponding network attack.

• **Remote access policy:** When a SCADA system is connected to an unaudited dial-up line or a remote login server, an attacker can easily access the business LAN, and ICS LAN inside the enterprise through the back door [7].

• **Distributed Denial-of-Service attacks:** Invalid sources and limited access control allow attackers to destroy Operational Technology (OT) systems by performing Distributed Denial-of-Service (DDOS) attacks on vulnerable unpatched systems [135]. DDoS attacks can be precisely divided into two forms: bandwidth consumption type and resource consumption type. They all require a significant amount of network and equipment resources through many legal or forged requests to achieve the purpose of paralyzing the network and the system.

• **Web application attacks:** Traditional OT systems, including HMIs and PLCs, are increasingly connected to networks and accessible anywhere via a web interface. As a result, unprotected systems are vulnerable to cross-site scripting and SQL injection attacks [128]. Web application attacks are popular APT attacks that are widely used by cybercriminals.

### 3.2 Introduction to APTs

An APT aims to exfiltrate information and control equipment via obtaining access to the victim’s nodes over a long time window [54]. An APT is challenging to mitigate due to combining multiple techniques, which demonstrate expansion in the quantity of IoT-based applications within the development of IoT [151]. Botnet of APT has become one of the most critical attacks in IoT networks, which utilizes malware to take control of the victim’s equipment connected to web services [167]. The computer dominated by an attack system is a botmaster, where the equipment under control of the botmaster is a bot. The botmaster can instruct a single bot simultaneously and work cooperatively for an individual task completion. With various bots under control of a botmaster, the
botmaster is able to inject large-scale activity in an IoT system, which is more harmful than a conventional malware attack [173]. The botnet attack life cycle can be summarized as spreading/injection, control, and application [57]. An APT can remain in disguise within the target system to prevent from being detected [33]. Therefore, this characteristic of APT has defined a remarkable open issue for security research. For instance, the study by Vinayakumar et al. [168] demonstrates a framework for botnet attack detection via investigating DNS services in the IoT of smart cities scenarios, which integrates DL algorithms to inspect DNS logs with motivation to reduce a false alarm rate. Sriram et al. [151] implement a DL-based approach to identify botnet attacks, which aggregates network data in IoT systems and extracts features among them such as connection log data. The proposed system contributes higher detection performance than normal ML algorithms. Moreover, Vinayakumar et al. [127] investigate a detection system for botnet attack-based domain generation algorithms and DNS homographs detection with DL models. Zero-day exploits combined with social engineering techniques result in almost undetectable behavior [155]. This means that APTs lead to critical damage and substantial financial loss due to an extended period and response costs to be able to identify them [101]. An APT attack primarily contains the following three characteristics:

1. **Advanced**: Attackers do not follow an immutable attack pattern but analyze the target network so as to formulate the most effective attack strategy exploiting zero-day vulnerabilities, phishing emails, and SQL injections, among others [16]. In addition to computer attacks, social engineering and psychology are also used to guide target network users into traps unknowingly and become the links in the attack chain [68].

2. **Persistent**: From the beginning of the attack until the attacker obtains the desired information, the duration of an APT attack is usually in months or even years [175]. Hackers have enough time to explore the victim network and adjust the attack strategy according to the actual situation to hide their traces better. Simultaneously, compared to a large amount of normal traffic, the data from the attacker is insignificant, which makes it difficult for network administrators and IDSs to detect [154].

3. **Threats**: APT attacks are complex and require the initiators to master many attack methods and computational theories so that it is difficult for individuals to complete such complex tasks. The funded hacker organizations are orderly and usually have the will of the organization or the country behind them [16]. After the target information is stolen, the hacker carries out follow-up work such as clearing traces, making it difficult to carry out the tracking investigation work, and the company or the country suffers enormous losses [121].

From the preceding characteristics, it is clear that the APT attack integrates the currently known attack methods, and according to the customized attack strategy, it infringes the target network for a long time, which is highly secretive and harmful. The six primary processes of an APT attack are shown in Figure 5. The yellow color blocks (e.g., Reconnaissance, Initial Compromise, Post Stage) indicate the initial and final stages of the APT attack, which mainly include information collection and trace spiritual work. The red color blocks (e.g., Lateral Movement, Pivoting, Data Exfiltration) represent the attack stages of APT, in which hackers gradually conquer the network domain and leak data. Hackers may change the sequence of the three attack stages according to the network environment.
Reconnaissance. In the Reconnaissance stage, the adversaries aim to collect enough information to prepare for the APT attack and develop appropriate attack strategies for the target network. The information collected includes social engineering information and the target network’s infrastructure information. Adversaries collect social information, hobbies, and social networking of users of the target network [187]. This information is used to assist in completing the Initial Compromise phase. The target network’s infrastructure information includes the models of network switches, routers, and the communication protocols used in the network [117]. Attackers use covert attack methods based on this information to ensure their security and construct a reasonable attack path to bypass the network administrators and IDS.

Initial Compromise. In this stage, the attacker uses the information collected in the Reconnaissance stage to attack the network user or the target network’s vulnerabilities to obtain the administrator privileges of the compromised computer. Then, they use this node to carry out large-scale attacks on the target network. The Initial Compromise stage mainly categorizes two forms. The first form is mainly for computer users [38]. After collecting enough social engineering information, adversaries attack network users through different techniques such as phishing emails or links to trick users into clicking in order for the attackers to gain administrator privileges. The second type aims at computer vulnerabilities. By understanding the computer’s operating system, patch version, and installed software, attackers use known vulnerabilities, and advanced hackers even use zero-day vulnerabilities to obtain root privileges [110].

Lateral Movement. In this stage, the APT attackers use the compromised node to obtain other computers’ credentials in the same network domain. Attackers use various methods to move laterally according to the actual situation in the network domain [158]. Commonly used techniques include pass-the-hash, pass-the-ticket, and Remote Desktop protocol [16]. It is worth mentioning that lateral movement and reconnaissance within the network domain can occur simultaneously. Unlike the original reconnaissance, internal reconnaissance mainly refers to the hacker’s activities inside the target network. After obtaining the administrator credentials, the adversaries obtain essential information such as the computer’s running process, IP, and port numbers. With the deepening of reconnaissance, attackers can also modify the attack strategy at any time, making APT attacks more difficult to detect.

Pivoting. For companies and organizations, a multi-location office has become a typical application scenario. Therefore, the internal network is often composed of two or more remote subnets responsible for different tasks. Each subnet has a domain controller and several user computers. The domain controllers are connected by a communication channel such as a VPN. When an APT attacker encounters the need to move laterally across different subnets, pivoting attacks become the most powerful tool [19].

Date Exfiltration. This stage mainly uses the session established by the previous attack for information and file return. To avoid being noticed by the IDS and anti-virus software, attackers usually use the tools that have been written to cut the files and then transfer them. Advanced hackers will take the different cut parts to different DNS servers and then collect the sliced file fragments to reduce the possibility of discovery [108].

Post Stage. When the hackers obtain all of the required information, the APT attack phase is over. The primary purpose of the Post Stage is to clean up the traces of APT attacks and prevent follow-up investigations [121]. During an APT attack, the attacker installs various malware on the compromised computer. Multiple logins and reconnaissance generate log files and browsing records. Therefore, cleaning up these traces can well hide the APT attack and avoid tracking investigation.
3.3 Attack Analysis with Threat Modeling

Threat modeling is a systematic way to help security experts, software engineers, and organizations determine the assets, structure, and potential vulnerabilities of target systems and prevent implied attacks [160]. The IIoT, specifically ICS, confronts significant security challenges due to slow patching processes, unsafe protocols, and other security problems, leaving a relatively open window for attackers to exploit vulnerabilities. For example, Industroyer, a malware framework that was discovered in 2016, targeted the electric grid in Ukraine’s capital, causing a short-term power outage in that area [1]. Therefore, threat modeling can be a useful process that can optimize network security by defining objectives. Threat modeling is vital for IIoT systems. In this article, the PASTA model is reviewed in respect to IIoT systems. As shown in Figure 7, there are seven stages of PASTA, including defining business objectives, defining the technical scope, application decomposition, threat analysis, vulnerable detection, attack enumeration, and impact analysis [144].

Figure 8 shows the high-level architecture of an ICS. As noted, an ICS contains four principal components: control and sensing systems, data services, asset management, and the institution’s private network(s) [102]. Control and sensing systems utilize on-site hardware to collect data from the environment and operate the overall network [84]. This system is similar to the perception layer in Figure 3. The data collected from the control and sensing systems will be stored and managed. Asset management handles and displays the data collected by sensors and actuators that form links with the organizations’ private network. The network devices and typologies in Section 2 with devices (e.g., network cameras, PLC, RTU, and HMI) are connected to the ICS LAN and the business LAN. Various protocols (e.g., S7, Modbus, Distributed Network Protocol 3 (DNP3),
EtherIP, HTTP, FTP, SSH, Telnet, and UPnP) can be used for the sensing components of the control system. The application layer utilizes data services such as SQL, SSH, and HTTP. However, these services can be exploited by attackers as shown in Figure 6. Moreover, control devices like PLCs may use mainstream operating systems like Windows or Linux, thereby increasing the threat surface and the vulnerabilities to the level of an entire enterprise’s digitally controlled operating environment [4].

ICS decomposition is shown in Figure 9, which illustrates more detailed structures such as the hardware, software, and entry points. Control systems are composed of multiple hardware components, including PLCs, RTUs, SCADA devices, or distributed control system devices. Data within control systems appear as raw ICS-based data (e.g., serial communication), ICS-based network traffic (e.g., DNP3, Modbus, and EtherIP), and traditional network traffic (e.g., TCP, UDP, ICMP, and ARP) [102]. The data flows from these networks into the management component of the current control system. Several services are deployed in the control system to handle the raw data from control systems, such as traditional and SCADA servers.

Either the raw data from control systems or the processed data from control system management are fed into a remote data service, which may use SQL or cloud techniques. The structured data are transferred from the network’s collection point to the management process, where cybersecurity
is applied and further displayed on the dashboard in the HMI systems. By analyzing the dataflow in the ICS, assets can be identified as hardware (e.g., PLCs, RTUs, or network cameras) or software such as multiple services leveraged to manage the control systems and data collected from the control systems. Moreover, the entry points contain the control system devices, internal networks, and data servers, among which IoT devices are the most vulnerable components due to the lack of security protection compared to servers or PCs. The ICS will also be connected to internal private networks, resulting in the potential for a broader threat to surface. Nonetheless, as our technical scope is limited to external attacks on IIoT, this work will not focus on industrial networks’ internal attacks.

Threat analysis assesses the possible threats targeting the assets and identifies the most probable attack scenarios. As a consequence, ICS and SCADA systems are high-value targets for attackers. For example, in 2019, the power sector received 6% of all ICS and SCADA attacks and incidents in the top 10 industries [6]. As pointed out by IBM in 2019 [3], attacks targeting Windows Server Message Block protocol can be automatically implemented, making it easier for low-level attackers to compromise devices. Commodity downloaders, such as Emotet and TrickBot, are often leveraged by attackers to execute the malware on victims’ machines. Meanwhile, PowerShell is frequently used to download attack tools and native functions, such as PSEexec or Windows Management Instrumentation, which are also exploited to help malicious users move laterally, which can be hard to detect.

A significant number of vulnerabilities exploit improper authentication or excessive privileges. By this we mean that too much privilege is assigned so we may keep “excessive privilege,” among which 64% [6] can be utilized remotely by attackers. These vulnerabilities involve permissions, privileges and access controls, improper input validation, improper restriction of operations within the bounds of memory buffers, path traversal, information exposure, improper access control, command injection, SQL injection, scripting, and improper authentication. In addition, 82% of these vulnerabilities exploit networks attack vectors; hence, network equipment is the crucial component in delivering commands among ICS devices [6]. This equipment vulnerability offers ICS attack surfaces consisting of personal computers on internal networks, IoT devices, control system devices, HMIs, and databases.

4 INTRUSION DETECTION APPROACHES IN IOT

This section provides a review of IDS for IoT, emphasizing ML approaches. IDSs can be categorized into several types based on the detection mechanism, namely anomaly based, signature based, hybrid, collaboration, and specification [182]. The anomaly-based, signature-based, hybrid IDS, and collaborative methods are introduced in the subsequent sections. Specification-based approaches require a collection of rules and thresholds to determine network component behaviors. When network behavior deviates from specification definitions, specification-based approaches kick in to detect intrusions [182]. The survey of Liu et al. [92] points out that a specification-based IDS in a smart grid can achieve superior performance. However, only a few works investigate the integration of specification-based approaches and MLs. Therefore, we do not focus on specification-based IDS in this review. Table 4 summarizes the different approaches to implement network intrusion systems [141] (e.g., statistical, data mining, and ML), among which ML-based methods [153] are used in hybrid detection systems [61].

4.1 Signature-Based Methods

A signature detection system differentiates malicious from standard traffic patterns or application data [69]. If the network behavior matches a stored pattern or signature of nefarious code, it is marked as abnormal. Thus, signature detection can identify attacks, but only if a signature (e.g.,
Table 4. IDS Techniques

| IDS Technique | Ref. | Attack | Benefits | Open Issues |
|---------------|------|--------|----------|-------------|
| Signature     | [69] | DoS    | Implements two types of DoS | Low performance |
|               | [106]| Traffic analysis | Low computing time | Real-time attack detection |
| Anomaly       | [45] | Wormhole | Wormhole rarely discussed | Low positive detecting |
|               | [94] | Sink hole | Promising performance | Identify attack earlier |
|               | [97] | DoS | 50% of the computational costs | Long delay |
| Hybrid        | [31] | Sink hole | Low false prediction | More types of attack detection |
|               | [163]| DoS  | 99.06% detection accuracy | Time consuming |
| Collaborative | [83] | DoS, Probe, R2L U2R | Low false alarm; efficient | Vulnerability to various data characteristics |
|               | [21] | Distributed attacks | Low workload | Require RAM increase |

label) for the attack is available. Hence, the method performs poorly in cases representing a new kind of attack [182].

The minimal computing power and memory limitations of IoT devices combine to create a security challenge compared to traditional network and computer security systems. The study of Oh et al. [113] shows a comparison between packet payloads and attack signatures systems while considering the difference in the computational cost of the two detection systems. Consequently, the authors demonstrate a lightweight security system using a pattern-matching engine to detect malicious code. The engine runs on resource-limited equipment by restraining memory usage of a simulated IoT system. Meanwhile, they present two innovative techniques called auxiliary shifting and early decision with motivation to alleviate degradation of performance given the constraint on sensor-level computational power and available memory. Based on these proposed techniques, the number of matching operations on resource-constrained systems, such as an IoT network, decreases, resulting in enhanced efficiency under constrained conditions.

Mughal et al. [106] demonstrate a lightweight digital signature approach to ensure reliable communication between smart equipment IoT networks with a reduced number of operations. The proposed method ensures security via guarding against traffic analysis attacks in IoT systems. A DoS detection architecture is demonstrated for the 6LoWPAN protocol for low-power lossy networks [107].

4.2 Anomaly-Based Methods

An anomaly detection system compares a captured pattern in a data stream to pre-stored baseline patterns of known threats. If the patterns match, action is taken according to the operational needs of the time. However, the downside of anomaly detection is the potential for inevitable false alarms. Based on applied techniques, anomaly-based intrusion detection methods can be categorized according to their use of learning, statistics, and miscellaneous techniques [156]. In a statistics-based approach, network traffic activities capture and create a profile representing the random behavior of network traffic. This profile takes various essential features into account (e.g., traffic rate, number of packets, connections, multiple IP addresses). The anomaly detection procedure for network traffic utilizes two datasets. One dataset contains the current observed profile, and the other is a previously trained statistical profile. As network events occur, the existing profile is determined, and a quantitative value is calculated by comparing the two actions. Thus, IDSs can figure out anomalies based on the calculated scores. The statistics-based methods lead to increased detection
accuracy. However, the downside of statistical methods is that malicious users could hack into the system by training the system and its parameters by injecting malicious code.

The category of miscellaneous detection techniques consists of all approaches not included in the statistical and ML groups and includes using such approaches as control flow graphs [169], finite automata [30], and description languages [176].

For instance, the study of Hussein and Zulkernine [67] provides a framework to determine intrusion based on the general-purpose Unified Modeling Language (UML). The authors design a UML profile called UMLintr that allows software developers to specify intrusions using UML notations extended to suit the context of various intrusion scenarios. The framework uses the expressiveness of UML and eradicates the requirement of using attack languages. It is unnecessary to study UML for attack descriptions, thus reducing developers’ efforts in specifying intrusion scenarios. Wressnegger et al. [176] introduce a description language (e.g., n-grams) for intrusion detection. They show both anomaly detection and classification based on n-grams. In addition, they develop criteria for utilizing data using different schemes and applying the defined criteria to web intrusion detection. Although miscellaneous detection techniques are flexible and scalable, they are not effective for high quality and high volumes of data due to time-consuming data management caused by a low-power and limited memory environment [52]. Lately, several works have deployed anomaly techniques to defend against attacks in an IoT system, including wormhole attack, sinkhole attack, and DoS, among many others. For instance, the study of Deshmukh-Bhosal and Sonavane [45] investigates an anomaly technique based framework for wormhole attack detection, which is rarely discussed in recent literature. The authors demonstrate wormhole attack at the 6LoWPAN adaption layer of the RPL network that is mitigated by an implemented IDS in Contiki OS. Liu et al. [94] introduce a PRDSA scheme based on probe route to prevent sinkhole attack and ensure security for IoT systems. The PRDSA framework can be utilized for detecting, bypassing, and locating sinkhole attack simultaneously. Furthermore, an IDS built on an anomaly technique is studied by Lyu et al. [97] to address DoS attack in the IoT. IoT systems are vulnerable due to DoS attacks that are attacked by malicious users to deliver a large number of valid data. Thus, the authors propose a selective authentication-based geographic opportunistic routing framework to resist DoS attacks in the IoT that performs about 50% of computational cost and provides a reliable data distribution.

In recent years, ML algorithms have emerged as a tool to assist in anomaly-based IDSs. ML techniques are used to build explicit or implicit models that utilize pattern analysis to classify data. An ML-based network intrusion system can change its execution strategy as it obtains new information [52]. There are several ML algorithms used in anomaly-based detection systems, including SVM, Bayesian, neural network, clustering, and outlier detection [52, 156]. The study of Ghazal et al. [56] demonstrates a comprehensive review introducing ML-based schemes targeting IoT for smart healthcare. The main disadvantage is the need for relatively expensive computation resources to perform the necessary data processing.

4.3 Hybrid Methods

As for the hybrid detection system, it combines the signature-based and anomaly-based approaches to overcome their drawbacks and benefit from their advantages [147]. Hence, hybrid detection systems can synthesize the benefits of two methods such as the detection of “zero-day”attacks and the detection of signatures of known attacks. The traditional IDS is difficult to deploy straightforwardly in IoT networks because of various communication schemes, protocols, technologies, and particular services. Meanwhile, the hybrid-based IDS is able to adapt techniques and services in real time, which is a serious issue in the conventional IDS [163]. Venkatraman and Surendiran [163]
design a hybrid IDS based on a timed automate controller approach to detect DoS attack, control hijacking attack, zero-day attack, and replay attack in IoT environments with promising accuracy (e.g., 99.06%). Singh and Venkatesan [147] introduce hybrid techniques, namely using Gaussian mixture clustering with Random Forest (RF) classifiers, as well as using K-means clustering with RF classifiers, to detect intrusions. The authors report that this proposed hybrid approach decreased the false alarm rate to 0.04%. Cervantes et al. [31] demonstrate a hybrid IDS, called INTI, which was designed to detect sinkhole attacks in the routing services within an IoT network. INTI links anomaly-based concepts and specification-based methods to monitor and audit packets between nodes and extracts reputation and trust features for node evaluation.

4.4 Collaborative Methods

Collaborative IDSs attract attention for IoT applications. They differ from the other three types of methods. Collaborative methods do not need a high demand for resources and reduce delay in identifying suspicious activities since they monitor and collect abnormal acts. Collaboration between IoT equipment allows obtaining knowledge from various host and network equipment to result in promising detection performance [162]. The study of Arshad et al. [21] demonstrates a collaborative IDS, namely COLIDE, to identify attacks in IoT networks, which allows an efficient detection with low latency via collaboration among sensors and devices with limited resources in IoT systems. Li et al. [83] present a collaborative IDS to boost detection accuracy, which integrates a semi-supervised ML model to address the missing label problem. It is possible to observe unlabeled network samples due to the expensive cost of labeling numerous instances in a network. The upside of a collaborative IDS is reported to be a lower false alarm rate and efficient performance with unlabeled samples.

5  ML IN IOT SECURITY

ML can be utilized to implement a data-driven intelligent attack detection platform for IoT systems [136]. In this section, we study various ML-based approaches that are used to detect network intrusions in IoT applications and categorize them as supervised ML, DL, and unsupervised ML algorithms as shown in Tables 5, 6, and 7, respectively. Among the research considered in this work, supervised ML methods are widely used to guarantee accuracy and efficiency, whereas unsupervised methods are not as commonly used for intrusion detection in IoT networks. Meanwhile, DL approaches confront issues such as higher requirements of computation resources and longer response time for prediction when compared with ML algorithms.

5.1 Supervised ML Methods for Network Intrusion Detection

AdaBoost stands for Adaptive Boosting, the first practical boosting algorithm, which is used widely in various applications [137, 165]. The study of Rachmadi et al. [123] introduces an IDS based on the AdaBoost model for DoS attack detection. The work applies a public IoT dataset MQTTset for evaluation that achieved up to 95.84% overall accuracy. Meanwhile, Wahla et al. [170] present a framework with AdaBoost for Low-Rate One-Class Denial-of-Service (LRDoS) attack detection, which is more difficult to identify compared to conventional DoS attack. Moreover, the proposed approach is adjusted according to sample weights, which tackles imbalanced dataset issues. Under an NS2 simulation-based test environment, the presented method has a 97.06% detection rate for the LRDoS attack.

Decision Tree (DT) algorithms depend on some pre-conditions and select a univariate split for the root of the tree and recursively repeat the process [134]. Pruning reduces the size of trees and is performed after a complete tree has been built. The study by Shafiq et al. [142] shows that the DT-based detection framework achieves up to 99.99% accuracy to identify Bot-IoT attacks using the
Table 5. Summary of ML Algorithms in IoT

| ML     | Ref. | Attack                                      | IoT Dataset   | Benefits                  | Open Issues                             |
|-------|------|---------------------------------------------|---------------|---------------------------|-----------------------------------------|
| AdaBoost | [123] | DoS                                         | MQTTset       | High accuracy             | Apply other ensemble models             |
| AdaBoost | [170] | LRDoS                                       | Private       | Optimizes AdaBoost        | Evaluate on real networks               |
| DT     | [142] | Botnet                                      | Bot-IoT       | 99.99% accuracy           | Apply other research                    |
| KNN    | [81]  | DoS, DP, MC, MO, SC,Spying, WS              | DS2OS         | 99.99% detection rate     | Apply other research                    |
| LR     | [63]  | DoS, DP, MC, MO, SC, Spyng, WS              | DS2OS         | High accuracy             | Build a robust algorithm                |
| LR     | [130] | Brute force, Broker Spoofing, and Malformed MQTT Packets | Private | Adapts to new schemes    | Define more event patterns              |
| LR     | [44]  | Bot                                         | CUT-13        | Detects unknown attack    | Long time convergence                   |
| RF     | [63]  | DoS, DP, MC, MO, SC, Spying, WS             | DS2OS         | High accuracy             | Build a robust detection algorithm      |
| RF     | [17]  | Blockhole and DoS                           | Private       | Crosses network layers    | Improve detection performance          |
| RF     | [63]  | DoS, DP, MC, MO, SC, Spyng, WS              | DS2OS         | High accuracy             | Build a robust detection algorithm      |
| SVM    | [63]  | DoS, DP, MC, MO, SC, Spyng, WS              | DS2OS         | High accuracy             | Focus on real-time data                 |
| SVM    | [109] | EAVESDROPPING, DoS, Spoofing, Man-in-middle | Private | 7-ms detection time      | Overhead of system collaboration        |
| SVM    | [70]  | BASHLITE and Mirai                          | N-BaIoT       | Metric reflecting security analysis | N/A                                     |
| XGBoost | [172] | Vulnerability exploiting, malware infection, abnormal operation, and memory leak | Private | Test under real IoT system | Improve diversity of generated DT       |

Table 6. Summary of DL Algorithms

| ML     | Ref. | Attack                                      | IoT Dataset   | Benefits                  | Open Issues                             |
|-------|------|---------------------------------------------|---------------|---------------------------|-----------------------------------------|
| DAE   | [82] | N/A                                         | N-BaIoT       | Less features used        | Reduce features                         |
| DBN   | [25] | DoS, Overflow, SSH, Brute Force, Malware, Cache poisoning | Private | Detects malicious activity inside the web | Improvement for standard               |
| FCN   | [118] | N/A                                         | Private       | Cost effectiveness        | Need more analyses                      |
| FCN   | [44] | Bot                                         | CUT-13        | Detects unknown attack    | Long time convergence                   |
| LSTM  | [15] | BASHLITE and Mirai                          | N-BaIoT       | Improves performance      | Need improvement for Scan and TCP flood |
| LSTM  | [89] | Abnormal data stream                        | Private       | Reduces regression error  | Need monitoring sensor status           |
| RNN   | [119] | Botnet                                      | Bot-IoT       | Robust and tackles        | Long training and response time         |
| RNN   | [58]  | Malware                                     | Private       | 94% accuracy              | Need a large DT                         |

ACM Computing Surveys, Vol. 55, No. 5, Article 105. Publication date: December 2022.
public dataset Bot-IoT. Furthermore, the study of Joloudari et al. [72] demonstrates 95.64% overall accuracy in detecting APT attacks in the NSL-KDD dataset via the DT algorithm, which deploys an early detection of these APT attacks. Thus, the proposed approach is suitable for APT attack detection due to APT long time presence in compromised systems.

A **K-Nearest Neighbor (KNN)** algorithm is a data classification method that estimates the likelihood that a data point will become a member of one group or another, depending on which group the nearest data point belongs. This means that a KNN classifier is a distance function, in effect an application of the Pythagorean theorem, which measures the difference or similarity between two instances [11]. The KNN ML approach is practical in several network categories (e.g., IoT, industry WLAN IoT, and self-designed networks), where each network could be affected by different attacks. From the literature [100], KNN has been deployed to detect several network attacks such as APT, remote tripping command injection, relay setting change, data injection, ransomware, and DoS. However, the KNN-based classification approach almost cannot detect R2L and U2R attacks since the amount of attack traffic is extremely low. Therefore, considering the promising performance of KNN for use in IoT networks, various works have proposed approaches based on this algorithm with the intent to mitigate network attacks [112].

The study of Manhas and Kotwal [100] introduces several ML algorithm implementations, including the KNN model MLP, DT, NB, and SVM, to detect an IDS in IoT systems. However, non-IoT-specific datasets are used to evaluate test performance in this literature. Oniani et al. [114] demonstrate a review of AI techniques that ensure security for IoT systems in medical settings, which indicates that KNN is one of the leading algorithms according to numerical results. Kumar et al. [81] design a distributed ensemble framework to identify intrusions via a fog computing technique to preserve IoT networks. It is worth noting an IoT-specific dataset, DS2OS, is used to evaluate the proposed system performance, which achieves up to a 99.99% detection rate.

The **Linear Regression (LR)** algorithm attempts to model the relationship between two variables by fitting a linear equation to observed data. Thus, one variable is considered an explanatory variable, whereas the other is a dependent variable [105]. LR demonstrates 100% accuracy to identify network attacks, which is applicable to various types of attacks such as DoS, probing, and Malicious Control (MC) [63]. The study of Roldán et al. [130] integrates ML algorithms (e.g., LR, support vector regression) and complex event processing techniques to identify various kinds of intrusions in a real-time healthcare IoT system. Moreover, the proposed approach demonstrates high performance for TCP, UDP and Xmas port scans, and DoS attack detection, with up to 100% accuracy. Roldán et al. [130] utilize a private dataset that assembled real-time data in a designed IoT network.

RF is an ensemble ML algorithm that consists of several DTs [120]. Each DT gives a prediction result and an overall result via voting by all DTs. For instance, it is assumed that three DTs are applied in RF for binary classification, class A and class B. Two of the trees give prediction results at a point belonging to class A, whereas one of three trees estimates the sample belongs in class B. Then RF considers the data as part of class A since the majority of members voted for class A. Multiple class classification follows in the same manner as binary classification. The RF algorithm

### Table 7. Summary of Unsupervised ML Algorithms in IoT

| Algorithm | Ref. | Attack | Dataset | Benefits | Open Issues |
|-----------|------|--------|---------|----------|-------------|
| DBSCAN    | [50] | N/A    | Private | Groups similar attacks effectively | Improve defense capability |
| K-means   | [44] | Bot    | CUT-13  | Detects unknown attack               | Long time convergence     |
| K-means   | [145]| Worm   | Private | 93% detection rate                  | N/A                       |

ACM Computing Surveys, Vol. 55, No. 5, Article 105. Publication date: December 2022.
is deployed to detect network attacks in Ethernet IoT and self-designed networks [63, 165]. The study of Amouri et al. [17] demonstrates a two-stage detection framework for blackhole and DoS attacks in mobile IoT systems. The authors collect data in a designed network and feed the data into RF and other ML models. The numeric results show an F1 score in the range of 93% to 99.36% in identifying the two attacks. In the work of Nõmm et al. [112], IoT botnet attack mitigation is investigated integrating feature selection and post hoc local analysis stages in RF and some other ML algorithm working procedures.

SVM is well known for its ability to effectively handle high-dimensional datasets, even if the number of dimensions is higher than the number of samples, while still maintaining its effectiveness. Since only a subset of samples, named support vectors, is used by SVM in its decision function. SVM is widely deployed in IoT networks to ensure system security and mitigate attacks. For instance, the study of Hasan et al. [62] utilizes several ML algorithms including SVM to detect DoS attack, Data Type Probing (DP), MC, Malicious Operation (MO), scan, spying, and Wrong Setup (WS). Nguyen et al. [109] introduce a novel framework, SeArch, to represent a collective NIDS in a cloud IoT network that integrates the SVM algorithm and other ML/DL models to mitigate the threats (e.g., eavesdropping, DoS, spoofing, man-in-middle) in IoT networks. Yang et al. [179] demonstrate a one-class SVM approach to detect attacks and protect IoT systems that reduces the requirement of memory and decreases computation time. Therefore, the proposed approach is able to be applied in a real-world IoT system that typically consists of resource-constrained devices. The study of Jan et al. [70] shows a lightweight attack detection system adopting the SVM algorithm to identify malicious users aiming to introduce suspicious data into an IoT network. SVM-based anomaly detection is summarized in a comprehensive review article [66].

XGBoost is an ensemble ML algorithm based on DTs that uses a gradient enhancement framework [34]. The study of Verma and Ranga [165] reports on an XGBoost-based classification method to mitigate network attacks with a detection performance of 97%. The authors combine XGBoost and Long Short-Term Memory (LSTM) together to construct a novel framework to ensure IoT device security [172]. It is worth noting that a real IoT system is established for performance evaluation. The proposed approach achieves promising performance for vulnerability exploiting, malware infection, abnormal operation, and memory leak.

5.2 DL for Network Intrusion Detection

**Deep Autoencoder (DAE)** consists of two symmetric multilayer feedforward networks (e.g., encoder and decoder).

DAE is used to reproduce the input at the output layer via the encoder and decoder. The number of neurons in the output layer is the same as the number of neurons in the input layer [183]. Researchers apply DAE in various fields such as dimension reduction, anomaly detection, and noise filtering [77]. The study of Lv et al. [96] demonstrates a neural network with three layers for intrusion detection that integrates DAE and some other ML algorithms. The authors utilize an improved dataset based on NSL-KDD via extracting samples in different layers (e.g., application layer, network layer, transport layer, and full layer). The highest accuracy is up to 97.83% with the proposed framework, which can reduce detection load and improve detection performance. Moreover, a lightweight DAE is introduced by Lahasn and Samma [82] that achieves high accuracy up to 99% under an IoT-specific dataset (N-BaIoT).

**Deep Belief Networks (DBNs)** are a class of the deep neural network that uses probability and unsupervised learning to produce output [64]. Each layer in the DBN learns the entire input, which means that the DBN works globally and regulates each layer in order. The network consists of a cluster of restricted Boltzmann machines, with nodes in each layer connected to all nodes in the previous and the next layer, whereas no connection exists in the same layer. DBN is modeled
after the human brain, making it more capable of recognizing patterns and processing complex information. Therefore, DBN algorithms are widely utilized to build network intrusion systems for IoT applications. The study of Zhang et al. [184] introduces a DBN-based network attack detection method combining a flow calculation and DL. A different work by Zhang et al. [185] presents a compact DBN-based framework for intrusion detection that is adjusted for complex IoT-integrated environment. A public network dataset (NSL-KDD) is used to evaluate the proposed approach that results in high detection performance for each class (e.g., DoS, R2L, Probe, U2R). However, the studies by Zhang et al. [184, 185] verify system performance based on common network datasets rather than an IoT-specific dataset. Balakrishnan et al. [25] introduce an enhanced DBN model to adopt current cyberattacks with more serious alarming in IoT networks that is compared with conventional IDS approaches. The study demonstrates that the DBN-integrated framework kept checking attacks (e.g., DoS, Overflow, SSH Brute Force, Malware, and Cache poisoning) based on DBN model obtained knowledge.

A **Fully Connected Network (FCN)** contains fully connected layers where all inputs from one layer are connected to each activation unit in the previous layer [86]. Fully connected neural network algorithms have proven effective at network intrusion detection with promising performance under different network types. A DNN model consists of one input layer, two hidden layers, and one output layer. The three layers are fully connected, which means that neurons in each layer have connections to all active neurons in the previous layer. Assuming that there are m neurons in layer $l - 1$. Fully connected neural network algorithms are extensively researched to detect network attacks [35, 44, 48, 63, 74, 122, 164, 166]. Specifically, the study of Bokka and Sadasivam [28] proposes a DNN-based approach for intrusion detection in a smart home IoT network that resulted in 99.42% accuracy. The study of Park et al. [118] demonstrates a use case on a smart factory deploying a DNN-based intrusion detection approach that is a context-sensitive-based system. The authors collect data and utilize it for an ML model to train and test. The approach is applied into a real company for a test that has been proven to be a cost-effective IDS. Meanwhile, the dataset is private, which is difficult for other researchers to access. Daya et al. [44] present a two-stage IDS BotChase targeting bot attack that integrates unsupervised ML algorithm K-means in the first stage and supervised algorithms (e.g., LR, DT, SVM, FNN) in the second stage. The BotChase can identify bots relying on various protocols, which achieves a robustness system to detect unseen attacks. However, the BotChase takes a long time to converge.

A **Recurrent Neural Network (RNN)** is a type of neural network that takes sequence data as input and performs recursion in the direction of sequence evolution [181]. It is usually used to process sequence information such as strings, lists, tuples, byte arrays, and range objects. Like other neural networks, it has an input layer, an output layer, and a hidden layer. However, the value of the RNN’s hidden layer depends not only on the current input but also on the hidden layer result of the last input [181]. Popoola et al. [119] introduce a stacked RNN integrated framework to detect botnet attack in smart home IoT networks that aims to identify attacks in an extremely imbalanced dataset Bot-IoT. The performance results show a robust system proposed that addresses an overfitting issue. Moreover, the study by HaddadPajouh et al. [58] demonstrates a malware attack detection system based on RNN as a classifier that targets ARM-integrated IoT systems. The authors collect samples as a dataset for RNN model training and testing that consists of 280 malware and 271 normal documents. Finally, a promising detection performance is presented in the evaluation section, in terms of 98% accuracy.

Intending to avoid long-term dependency issues, LSTM is a special type of RNN [65]. It is used in classifying, processing, and making predictions based on time series data, noting that there can be lags of unknown duration between important events in a time series. LSTM remembers
information for long periods with their typical behavior. The study by Elmasry et al. [48] demonstrates three DL algorithms (e.g., DNN, LSTM-RNN, and DBN) to evaluate the difference of IDS performance, which reduces the false alarm rate by 1% to 5% and the boosted detection rate by 4% to 6% using two public datasets (NSL-KDD and CICIDS2017). Alkahtani and Aldhyani [15] demonstrate a Convolutional Neural Network (CNN) and LSTM hybrid framework for botnet attack detection (BASHLITE and Mirai) that tackles the insufficient resource issue for devices in IoT networks. Meanwhile, the proposed approach increases botnet attacks accuracy, up to 90.88% under an IoT-specific dataset (N-BaIoT). Moreover, the study of Liu et al. [89] presents an LSTM model for detecting and correcting abnormal stream data in IoT networks that ensures a stable and robust IoT application with real-time observing and correcting function. The authors utilize a private dataset with temperature data stream in it, consisting of 96,453 samples collected from sensors.

5.3 Unsupervised ML for Network Intrusion Detection

Density-Based Spatial Clustering of Applications with Noise (DBSCAN) is an unsupervised learning method that is well known for clustering samples based on their density and identifying outliers located in low-density areas [138]. The studies by Chen et al. [35] and Daya et al. [44] illustrate a DBSCAN algorithm to detect network intrusion. The study by Ghallab et al. [55] demonstrates the DBSCAN-integrated model for outlier determination on IoT applications that boosts data quality. Furthermore, the study by Fu et al. [50] introduces classifying attack categories with motivation to address complicated, various source, and arranged attacks in IoT networks. The K-means clustering algorithm is an unsupervised ML method that originates from a vector quantization method in signal processing [14, 59]. The purpose of K-means clustering is to divide n points into k clusters so that every point belongs to the cluster corresponding to the nearest mean. K-means are usually applied to the fields of vector quantization, cluster analysis, and feature learning. K-means-integrated methods are presented in the work of Daya et al. [44] for attack detection. The study by Tsang et al. [159] investigates the development of a knowledge structure combining blockchain and IoT. The authors utilize K-means to analyze intra-cluster relations among samples in each cluster. Shukla [145] presents three innovative IDSs for IoT networks targeting worm attacks detection, including K-means-based IDS, DT-based IDS, and a hybrid framework consisting of K-means and DT. The numeric results show that the hybrid approach performs the highest accuracy and reduced false prediction critically. The study by Daya et al. [44] shows a two-stage IDS integrating the K-means algorithm in the first stage to ensure detection performance and detection effectiveness.

5.4 ML Defense Methods Statistic Results in Attack Detection

Numerous literature is reviewed where popular AI methods are applied for network intrusion detection. Section 5.1 lists works that have been reviewed for the supervised ML model, Section 5.2 reviews the literature using DL algorithms for security in IoT platforms, and Section 5.3 presents two unsupervised ML algorithms (K-means and DBSCAN) for intrusion detection in IoT networks. The statistical results for the ML-applied frequency are demonstrated in Figure 10, where 10 works use the FCN-based approach for detection, which is the most widely utilized frequency. Moreover, supervised ML approaches are widely used to address network intrusion over unsupervised ML algorithms and DL algorithms. In respect to unsupervised ML algorithms, there are limited works deploying attack detection in IoT networks. This work studies K-means and DBSCAN algorithms for ensuring security in IoT networks. Unsupervised ML algorithms are typically integrated with supervised AI models for intrusion detection in IoT platforms that are not conventionally utilized.
independently to identify attacks in IoT systems. In terms of detection performance among supervised ML algorithms and DL algorithms, ML algorithms have promising performance (e.g., 99.99% by DT in the work of Shafiq et al. [142]), whereas DL algorithms demonstrate a little bit lower performance (e.g., 94% in the work of HaddadPajouh et al. [58]) in intrusion detection in IoT systems. Regarding time complexity and demanding of resources, DL algorithms suffer from computational complexity and long training times [44]. Therefore, testing procedure efficiency needs to be considered when using DL algorithms [58].

5.5 IoT Dataset Introduction

The IoT-specific dataset is one of the most critical roadblocks in IoT security since there are quite limited public datasets available. Meanwhile, it is demanding and time consuming to deploy an IoT network to collect data and generate a private dataset. This section introduces several public IoT-related network intrusion datasets and presents private datasets created and utilized in existing works. The following content contains public datasets introduced, attack types, and features extracted, and Table 8 further summarizes the attributes of IoT intrusion detection datasets:

- **TON-IoT**: TON-IoT is designed for the AI-based IDS among the Industry 4.0 and IIoT environments [8]. It could be utilized to evaluate or validate the efficiency and intrusion detection performance of the AI models. The testbed includes a realistic large-scale network that is deployed by multiple virtual machines and sensors. Numerous attack techniques, including DoS, DDoS, and ransomware, against web applications, IoT gateways, and computer systems across the IoT/IIoT network are implemented within the testbed.

- **Bot-IoT**: The Bot-IoT dataset blends real IoT traffic with diverse attack traffic, most notably the botnet, to address the shortcomings of existing related datasets in terms of collecting total network traffic and attack diversity [80]. The raw traffic in PCAP format and the processed traffic used for ML in CSV format are released to the public for a variety of purposes. Additionally, these files are grouped into subcategories based on the attack types for convenience of labeling.
### Table 8. Summary of IoT Datasets

| Dataset         | Year | PA | Attack Traffic                          | Metadata | Format | Realistic |
|-----------------|------|----|------------------------------------------|----------|--------|-----------|
| MAWILab [2]     | 2010 | N  | Attack, Special, Unknown                 | N        | Tabular| Y         |
| CTU-13 [53]     | 2014 | Y  | Botnet, C2, Background                   | Y        | Packets,Malware| Y |
| N-BaIoT [104]   | 2018 | Y  | Bashlite, Mirai                          | N        | Tabular| Y         |
| DS2OS [116]     | 2018 | Y  | DoS, MC, MO, Spying, WS, Scan, DTP       | N        | Tabular| N         |
| Bot-IoT [80]    | 2019 | Y  | DDoS, DoS, OS and Service Scan, Keylogging, Data exfiltration | Y | Packets, Tabular| Y |
| TON-IoT [8]     | 2021 | Y  | Backdoor, DDoS, DoS, Injection, man-in-the-middle, Password, Ransomware, Scanning, XSS | Y | Packets, Tabular| Y |
| MQTTTest [123]  | 2021 | Y  | SlowTe, Brute force, Malformed data, Flooding, DoS attack | Y | Packets, Tabular| Y |
| AposematIoT-23 [139] | 2020 | Y  | Botnet, C2, Background                   | Y        | Packets, Flow| Y |
| Edge-IoTset [49]| 2022 | Y  | DoS/DDoS attacks, Information gathering, Man-in-the-middle attacks, Injection attacks, Malware attacks | N | Tabular| N |

PA: Publicly available.

- **MQTTset**: The MQTT dataset focuses on intrusions against the MQTT protocol, which is a standard application protocol for IoT networks [123]. The network traffic is gathered from a variety of real-life sensors. The dataset covers five attack types: SlowTe (a novel DoS attack), brute-force authentication, corrupted data, flooding, and DoS, among which brute-force authentication can be considered as an APT attack. There are 33 features available, including several TCP head capabilities and MQTT protocol characteristics.

- **CTU-13**: The CTU-13 dataset seeks to collect a large volume of traffic from real-world IoT networks, as well as background and botnet intrusions [53]. More than 90 IoT devices and 13 botnet viruses are used to generate realistic network traffic and intrusions. The dataset contains four types of attacks: botnet, C2, normal, and background. C2 is one of the APT stages. Argus is used to extract features from the extremely large PCAP files.

- **N-BaIoT**: Meidan et al. [104] establish the N-BaIoT dataset by configuring nine IoT devices. Four types of attacks are used: reconnaissance, man-in-the-middle, DoS, and botnet malware. Botnet attacks also include the establishment of a C2 channel; thus, reconnaissance, man-in-the-middle attacks, and the part of the botnet are considered APT attacks. In addition, 115 features are extracted from PCAP files, including packets, stream, and time-frame features.

- **DS2OS**: The DS2OS dataset was first introduced by Aubet and Pahl [116] and generated using the **Distributed Smart Space Orchestration System (DS2OS)** in a virtual IoT-integrated platform. DS2OS consists of several popular IoT-related intrusions. The whole architecture is a collection of different micro-services in an IoT environment that communicates via MQTT protocol. There are 347,935 normal observations and 10,017 malicious observations in this dataset. There are seven different types of attack traffic, including DoS, MC, MO, Probe, Scan, Spy, and WS.
- **Edge-IIoTset**: This is a realistic dataset of IoT and IIoT studying what is applicable to design centralized MLs and federated learning algorithms. It consists of 14 threats that are grouped into five classes, including DoS/DDos, information gathering, man-in-the-middle, injection, and malware. Additionally, 61 additional features are extracted from a variety of sources (e.g., alarms, logs, network traffic) based on 1,176 previously discovered features [49].

- **Aposemat IoT-23**: This is a dataset aiming for IoT applications, and it was introduced in 2020, with data captured from 2018 to 2019. It is composed of data collected from 20 malware IoT devices and 3 normal IoT devices [139]. It is critical to note that the benign traffic was collected from real equipment (e.g., an LED lamp, an Amazon Echo home intelligent personal assistant, and a smart doorlock) rather than simulations.

- **MAWILab**: This dataset contains four classes including normal traffic, anomalous, suspicious, and notice. The dataset with numerous samples such as numeric values, discrete data, IP addresses, and identification numbers is widely used for anomaly detection research. In addition, with the motivation of understanding anomaly detection, MAWILab makes use of two separate anomaly identification methods, including a straightforward predictive algorithm and a taxonomy of backbone traffic suspicious data [2].

Private IoT datasets are generated and applied for security research in several works [17, 58, 118, 130, 172]. To be specific, Roldán et al. [130] indicate that samples are extracted from a normal network scheme to generate a dataset for ML algorithms using. The private dataset consists of normal traffic, background, and attack samples [130]. Moreover, the study by Amouri et al. [17] deploys dedicated sniffers to assemble network traffic as a dataset from network layer and MAC layer in a designed Open Systems Interconnection based network. Wang and Lu [172] first built an abnormal framework call dataset collected in four intrusion scenes. Meanwhile, Wang and Lu [172] indicated that people can contact them for accessing the private data using an email address left in their work. Furthermore, the study by Park et al. [118] utilizes a composed dataset with host features and flow features collecting data from sensors, network traffic, and system resource logs on a smart factory. HaddadPajouh et al. [58] introduce a private dataset creation for benign and malware attacks separately. Benign samples are obtained from a system with Raspberry Pi II, whereas malware samples are captured via monitoring ARM-based malware in a virus analysis system. However, most works focus on performance of ML or DL algorithms in the topic about intrusion detection in IoT networks rather than introducing a private dataset creation.

### 6 OPEN ISSUES, CHALLENGES, AND OPPORTUNITIES AGAINST APT ATTACKS AND COMMON NETWORK DETECTION

In this section, possible research directions are presented to increase the use of ML techniques to mitigate common issues and opportunities (e.g., updated attack detection, IoT data characteristic, and ML algorithm selection and configuration [126, 143]) in attack detection and APT attack open issues and opportunities (e.g., lack of a dedicated APT attacks dataset, adversarial machine learning (AML)-based attacks and detection, and combing with malware detection) in IoT systems. Meanwhile, the anomaly detection approach proves to be effective in various attacks with encouraging performance, but it is not applied widely for APT attacks. We demonstrate promising opportunities for ATP attack detection using anomaly detection.

#### 6.1 Common Challenges and Opportunities in Network Intrusion

##### 6.1.1 Updated Attack Detection

Billions of electronic devices (e.g., sensors) and machines are being connected to IoT systems. This connectivity trend is anticipated to continue well into the future, especially regarding wireless IoT in applications such as smart cities. This means that each
piece of equipment added to the network has multiple chances to be a vector for zero-day attacks. Therefore, ML algorithms should have the ability to learn adaptively and continuously to alleviate these anticipated attacks given the scale of network entry points.

The current ML paradigm works in two steps: first, a specific training dataset runs an ML algorithm to construct a model; then, the model is used for its intended IoT application [36, 37]. The process of continuous ML is still in early development, so challenges exist in applying continuous learning to IoT. Silver et al. [146] demonstrate lifelong ML taking into account systems that can learn various tasks from one or more domains during their lifetime. The objective is to absorb learning sequentially to selectively apply that knowledge when learning a new scheme to form more refined assumptions and/or policies. Moreover, the authors suggest that the AI community should look beyond merely one-time learning algorithms to more seriously consider the nature of systems that can learn throughout their operational lifetime. Consequently, in the future, we can consider ways and means to deploy lifelong ML to identify cyber intrusion in the future in IoT.

6.1.2 IoT Data Characteristic. ML algorithms rely on data to train and generate an accurate model. Since the data are the basis of extracting knowledge, it is crucial to ensure the data’s high fidelity. Data quality, availability, and integrity play a critical role in AI algorithm training and testing. However, IoT systems generate high volume, high velocity, and different data varieties, sometimes referred to as the 3 V’s. Meanwhile, various types of equipment and devices are used to generate data that introduce data heterogeneity. Consequently, it is a challenge to ensure data authentication in IoT. However, ML algorithms show great promise in addressing these IoT security challenges.

6.1.3 ML Algorithm Selection and Configuration. AI algorithms each have particular characteristics, abilities, and limitations. Tables 5, 6, and 7 describe individual model benefits and open issues. For instance, the KNN-based approach has a high detection rate up to 99.99% using the DS2OS dataset, whereas DAE indicates that less features are applied in attack detection. There is currently no guideline on how to select AI algorithms for IoT. Therefore, users need to choose ML models carefully.

6.2 Challenges and Opportunities for APT Attack Detection

6.2.1 Lack of a Dedicated APT Network Intrusion Dataset. There are several attractive datasets for network intrusion detection investigation. For instance, KDD 99 is one of the most utilized in studying network IDSs [12, 47, 75]. KDD 99 is public, and it is a benchmark to evaluate performance between provided approaches. However, there is no public dataset including pure ATP attacks. Some popular datasets (e.g., NSL-KDD) contain several types of ATP attacks (e.g., U2R, R2L), whereas most of the malicious samples within the NSL-KDD dataset are DoS attacks. It is difficult to use them for APT studying, which is the biggest challenge for researching and analyzing. Furthermore, as APT attackers compromise hosts gradually, even packets sent by the same ports can have different labels. As APT attack records are already rare in the dataset, a detailed malware behavior analysis should be provided so that the dataset can be labeled more carefully to reduce false positives and enhance the IDS’s performance.

6.2.2 AML-Based Attack and Detection. One of the challenges of APT attacks is to bypass the defense systems without being discovered. Since AML aims to mislead the ML classifiers, many of current works focus on employing AML on network intrusion to circumvent ML-based security systems [90]. Sriram et al. [150] demonstrate that adversarial samples created via AML approaches such as Jacobian-based Saliency Map Attack and the Fast Gradient Sign method can considerably affect ML/DL-based NIDSs. Other research provides defense measures—for example, Vinayakumar
et al. [127] use a two-level DNN framework to detect fraudulent DNS domains generated by AML, and there are still tough issues to address, such as increasing the speed and effectiveness of AML training.

6.2.3 Combining with Malware Detection. Due to the fact that APT attacks require the submission of malware to establish C2 and data exfiltration tunnels, numerous studies have focused on applying malware detection to the APT process—for example, Sriram et al. [152] use an end-to-end DL approach to identify a variety of malware with varying file sizes. As a result, merging the detection methods of both sectors could be a promising direction for the future.

7 CONCLUSION

This survey article has reviewed the current literature related to attacks and their countermeasures concerning the IoT. More specifically, we have focused on ML-based methods currently being used to mitigate IoT network attacks. Following upon a general introduction to IoT and IIoT, security in IIoT, specifically ICSs, has been described. Common attacks and APT attacks in an IoT network have been presented alongside an attack taxonomy and the APT attack distribution in this taxonomy. Based upon these attack types, the PASTA threat model has been used to illustrate vulnerabilities and attack paths in IIoT networks. In response to various attack types, network intrusion detection methodologies have been summarized in the form of three categories: signature-based, anomaly-based, and hybrid approaches.

As a promising strategy to enhance the detection performance in mitigating attacks, ML-based methods have been presented by also focusing on anomaly-based and hybrid approaches to detect and classify attacks on IoT networks. ML algorithms have been studied and compared in terms of their detection performance under certain attack types. Finally, to help researchers who work in IoT, IIoT, ML, and cybersecurity, open issues and challenges for network intrusion have been discussed based on ML techniques alongside those for protecting IoT networks from APT attacks.

REFERENCES

[1] Rodika Tollefson. 2020. ICS/SCADA Malware Threats. Retrieved April 23, 2022 from https://resources.infosecinstitute.com/category/certifications-training/ics-scada/ics-scada-threats-threat-actors/ics-scada-malware-threats/.

[2] Romain Fontugne, Pierre Borgnat, Patrice Abry, and Kensuke Fukuda. 2010. MAWILab: Combining Diverse Anomaly Detectors for Automated Anomaly Labeling and Performance Benchmarking. In ACM (CoNEXT’10). Philadelphia, PA.

[3] IBM. n.d. X-Force Threat Intelligence Index 2020. Retrieved April 23, 2022 from XXX.

[4] Control Engineering. 2009. When Considering Controllersâ€™ Do Operating Systems Matter? Retrieved April 23, 2022 from https://www.controleng.com/articles/when-considering-controllers-do-operating-systems-matter/.

[5] Steve Morgan. 2018. Global ransomware damage costs predicted to hit $11.5 billion by 2019. Cybercrime Magazine. Retrieved April 23, 2022 from https://cybersecurityventures.com/ransomware-damage-report-2017-part-2/.

[6] Positive Technologies. 2019. ICS Vulnerabilities: 2018 in Review. Retrieved April 23, 2022 from https://www.ptsecurity.com/ww-en/analytics/ics-vulnerabilities-2019/.

[7] CISA. 2020. Overview of Cyber Vulnerabilities. Retrieved April 23, 2022 from https://www.us-cert.gov/ics/content/overview-cyber-vulnerabilities.

[8] Nour Moustafa. 2021. A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets. Sustainable Cities and Society 72 (2021), 102994. https://doi.org/10.1016/j.scs.2021.102994

[9] Zeeshan Abbas and Wonyong Yoon. 2015. A survey on energy conserving mechanisms for the Internet of Things: Wireless networking aspects. Sensors 15, 10 (2015), 24818–24847.

[10] Mohammed Riyadh Abdmeziem, Djamel Tandjouai, and Imed Romdhani. 2015. A decentralized batch-based group key management protocol for mobile Internet of Things (DBGK). In Proceedings of the 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing. IEEE, Los Alamitos, CA, 1109–1117.
ML-Enabled IoT Security: Open Issues and Challenges Under APTs 105:29

[11] Yash Agarwal and G. Poonmalatha. 2021. Analysis of the nearest neighbor classifiers: A review. In Advances in Artificial Intelligence and Data Engineering. Advances in Intelligent Systems and Computing, Vol. 1133. Springer, 559–570.

[12] Muaz Salam Al-Daweri, Khairul Akram Zainol Ariffin, Salwani Abdullah, and Mohamad Firham Efendi Senan. 2020. An analysis of the KDD99 and UNSW-NB15 datasets for the intrusion detection system. Symmetry 12, 10 (2020), 1666.

[13] Mohammed Ali Al-Garadi, Amr Mohamed, Abdulla Khalid Al-Ali, Xiaojiang Du, Ihsan Ali, and Mohsen Guizani. 2020. A survey of machine and deep learning methods for Internet of Things (IoT) security. IEEE Communications Surveys & Tutorials 22, 3 (2020), 1646–1685.

[14] Wathiq Laftah Al-Yaseen, Zulaika Ali Othman, and Mohd Zakree Ahmad Nazri. 2017. Multi-level hybrid support vector machine and extreme learning machine based on modified k-means for intrusion detection system. Expert Systems with Applications 67 (Jan. 2017), 296–303. https://doi.org/10.1016/j.eswa.2016.09.041

[15] Hasan Alkahtani and Theyazn H. H. Aldihyani. 2021. Botnet attack detection by using CNN-LSTM model for Internet of Things applications. Security and Communication Networks 2021 (2021), Article 3806459.

[16] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang. 2019. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE Communications Surveys Tutorials 21, 2 (2019), 1851–1877. https://doi.org/10.1109/COMST.2019.2891891

[17] Amar Amouri, Vishwa T. Alaparthy, and Salvatore D. Morgera. 2020. A machine learning based intrusion detection system for mobile Internet of Things. Sensors 20, 2 (2020), 461.

[18] Oxana Andreeva, Sergey Gordeychik, Gleb Gritsai, Olga Kochetova, Evgeniya Potselevskaya, Sergey I. Sidorov, and Alexander A. Timorin. 2016. Industrial Control Systems Vulnerabilities Statistics. Kaspersky. https://doi.org/10.13140/RG.2.2.15858.66241

[19] Giovanni Apruzzese, Fabio Pierazzi, Michele Colajanni, and Mirco Marchetti. 2017. Detection and threat prioritization of pivoting attacks in large networks. IEEE Transactions on Emerging Topics in Computing 8, 2 (2017), 404–415.

[20] Claudia Aradu. 2010. Security that matters: Critical infrastructure and objects of protection. Security Dialogue 41, 5 (2010), 491–514.

[21] Junaid Arshad, Muhammad Ajmal Azad, Mohammad Mahmoud Abbellatif, Muhammad Habib Ur Rehman, and Khaled Salah. 2019. COLIDE: A collaborative intrusion detection framework for Internet of Things. IET Networks 8, 1 (2019), 3–14.

[22] Bijoy Babu, Thafasal Ilyas, P. Muneer, and Justin Varghese. 2017. Security issues in SCADA based industrial control systems. In Proceedings of the 2017 2nd International Conference on Anti-Cyber Crimes (ICACC’17). IEEE, Los Alamitos, CA, 47–51. https://doi.org/10.1109/Anti-Cybercrime.2017.7905261

[23] Thar Baker, Muhammad Asim, Åine MacDermott, Farkhund Iqbal, Faouzi Kamoun, Babar Shah, Omar Alfandi, and Mohammad Hammoudheh. 2020. A secure fog-based platform for SCADA-based IoT critical infrastructure. Software: Practice and Experience 50, 5 (2020), 503–518.

[24] Thar Baker, Muhammad Asim, Åine MacDermott, Farkhund Iqbal, Faouzi Kamoun, Babar Shah, Omar Alfandi, and Mohammad Hammoudheh. 2020. A secure fog-based platform for SCADA-based IoT critical infrastructure. Software: Practice and Experience 50, 5 (2020), 503–518. https://doi.org/10.1002/spe.2688

[25] Nagaraj Balakrishnan, Arunkumar Rajendran, Danilo Pelusi, and Vijayakumar Ponnusamy. 2021. Deep belief network enhanced intrusion detection system to prevent security breach in the Internet of Things. Internet of Things 14 (2021), 100112.

[26] Elisa Bertino, Ashish Kamra, and James P. Early. 2007. Profiling database application to detect SQL injection attacks. In Proceedings of the 2007 IEEE International Performance, Computing, and Communications Conference. 449–458. https://doi.org/10.1109/PCCC.2007.358926

[27] Leyla Bilge and Tudor Dumitras. 2012. Before we knew it: An empirical study of zero-day attacks in the real world. In Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS’12). ACM, New York, NY, 833. https://doi.org/10.1145/2382196.2382284

[28] Raveendranadh Bokka and Tamilselvan Sadasivam. 2021. Deep learning model for detection of attacks in the Internet of Things based smart home environment. In Proceedings of the International Conference on Recent Trends in Machine Learning, IoT, Smart Cities, and Applications. 725–735.

[29] Philip J. Boyle and Shannon T. Speed. 2018. From protection to coordinated preparedness: A genealogy of critical infrastructure in Canada. Security Dialogue 49, 3 (2018), 217–231.

[30] Joel Branc, Alan Bivens, Chi Yu Chan, Taek Kyeun Lee, and Boleslaw K. Szymanski. 2002. Denial of service intrusion detection using time dependent deterministic finite automata. In Proceedings of the Graduate Research Conference. 45–51.

[31] Christian Cervantes, Diego Poplade, Michele Nogueira, and Aldri Santos. 2015. Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things. In Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM’15). IEEE, Los Alamitos, CA, 606–611.

ACM Computing Surveys, Vol. 55, No. 5, Article 105. Publication date: December 2022.
[32] Nadia Chaabouni, Mohamed Mosbah, Akka Zemmari, Cyrille Sauvignac, and Parvez Faruki. 2019. Network intrusion detection for IoT security based on learning techniques. *IEEE Communications Surveys & Tutorials* 21, 3 (2019), 2671–2701.

[33] Ping Liu, Lieven Desmet, and Christophe Huygens. 2014. A study on advanced persistent threats. In *Proceedings of the IFIP International Conference on Communications and Multimedia Security*. 63–72.

[34] Tianqi Chen, Tong He, Michael Benesty, Vadim Khotilovich, Yuan Tang, Hyunsu Cho, et al. 2015. xgboost: Extreme gradient boosting. *R Package Version 0.4-2* 1, 4 (2015), 1–4.

[35] Xiaoliang Chen, Baojia Li, Roberto Proietti, Zuqing Zhu, and S. J. Ben Yoo. 2019. Self-trained anomaly detection with hybrid unsupervised/supervised machine learning in optical networks. *Journal of Lightwave Technology* 37, 7 (2019), 1742–1749. https://doi.org/10.1109/JLT.2019.2902487

[36] Zhiyuan Chen and Bing Liu. 2018. *Lifelong Machine Learning* (2nd ed.). Synthesis Lectures on Artificial Intelligence and Machine Learning. Morgan & Claypool.

[37] Zhiyuan Chen, Nianzu Ma, and Bing Liu. 2018. Lifelong learning for sentiment classification. *arXiv preprint arXiv:1801.02808* (2018).

[38] Bernard Lee Jin Chuan, Mammeet Mahinderjit Singh, and Azizul Rahman Mohd Shariff. 2018. APTGuard: Advanced persistent threat (APT) detections and predictions using Android smartphone. In *Computational Science and Technology*, Rayner Alfred, Yuto Lim, Ag Asri Ag Ibrahim, and Patricia Anthony (Eds.). Springer, Singapore, 545–555.

[39] Michael W. Condy and Catherine Blackadar Nelson. 2016. Using smart edge IoT devices for safer, rapid response with industry IoT control operations. *Proceedings of the IEEE* 104, 5 (May 2016), 938–946. https://doi.org/10.1109/JPROC.2015.2513672

[40] A. Creery and E. J. Byres. 2005. Industrial cybersecurity for power system and SCADA networks. In *Record of Conference Papers Industry Applications Society 52nd Annual Petroleum and Chemical Industry Conference*. 303–309. https://doi.org/10.1109/PICCON.2005.1524567

[41] Kelton A. P. da Costa, João P. Papa, Celso O. Lisboa, Roberto Munoz, and Victor Hugo C. de Albuquerque. 2019. Internet of Things: A survey on machine learning-based intrusion detection approaches. *Computer Networks* 151 (2019), 147–157.

[42] Li Da Xu. 2011. Enterprise systems: State-of-the-art and future trends. *IEEE Transactions on Industrial Informatics* 7, 4 (2011), 630–640.

[43] Li Da Xu, Wu He, and Shancang Li. 2014. Internet of Things in industries: A survey. *IEEE Transactions on Industrial Informatics* 10, 4 (2014), 2233–2243.

[44] Abbas Abou Daya, Mohammad A. Salahuddin, Noura Limam, and Raouf Boutaba. 2020. BotChase: Graph-based bot detection using machine learning. *IEEE Transactions on Network and Service Management* 17, 1 (2020), 15–29. https://doi.org/10.1109/TNSM.2020.2972405

[45] Snehal Deshmukh-Bhosale and Santosh S. Sonavane. 2019. A real-time intrusion detection system for wormhole attack in the RPL based Internet of Things. *Procedia Manufacturing* 32 (2019), 840–847.

[46] Oliver Eigner, Philipp Kreimel, and Paul Tavolato. 2016. Detection of man-in-the-middle attacks on industrial control networks. In *Proceedings of the 2016 International Conference on Software Security and Assurance (ICSSA’16)*. IEEE, Los Alamitos, CA, 64–69.

[47] Charles Elkan. 2000. Results of the KDD’99 classifier learning. *ACM SIGKDD Explorations Newsletter* 1, 2 (2000), 63–64.

[48] Wisam Elmasry, Akhan Akbulut, and Abdul Halim Zaim. 2020. Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic. *Computer Networks* 168 (Feb. 2020), 107042. https://doi.org/10.1016/j.comnet.2019.107042

[49] Mohamed Amine Ferraq, Othmane Friha, Djallel Hamouda, Leandros Maglaras, and Helge Janicke. 2022. Edge-IoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications: Centralized and federated learning. *IEEE Access* 10 (2022), 40281–40306. https://doi.org/10.1109/ACCESS.2022.3136468

[50] Chen Fu, Yu Rui, and Liu Wen-Mao. 2021. Internet of Things attack group identification model combined with spectral clustering. In *Proceedings of the 2021 IEEE 21st International Conference on Communication Technology (ICCT’21)*. 778–782. https://doi.org/10.1109/ICCT52962.2021.9657991

[51] Sunanda Gamage and Jagath Samarabandu. 2020. Deep learning methods in network intrusion detection: A survey and an objective comparison. *Journal of Network and Computer Applications* 169 (2020), 102767.

[52] Pedro García-Teodoro, Jesús Díaz-Verdejo, Gabriel Maciá-Fernández, and Enrique Vázquez. 2009. Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security* 28, 1–2 (2009), 18–28.

[53] S. García, M. Grill, J. Stiborek, and A. Zunino. 2014. An empirical comparison of botnet detection methods. *Computers & Security* 45 (Sept. 2014), 100–123. https://doi.org/10.1016/j.cose.2014.05.011

[54] Ibrahim Ghafir and Vaclav Prenosil 2014. Advanced persistent threat attack detection: An overview. *International Journal of Advances in Computer Networks and Its Security* 4, 4 (2014), 5054.
Haitham Ghallab, Hanan Fahmy, and Mona Nasr. 2020. Detection outliers on Internet of Things using big data technology. *Egyptian Informatics Journal* 21, 3 (2020), 131–138.

Taher M. Ghazal, Mohammad Kamrul Hasan, Muhammad Turki Alshurideh, Haitham M. Alzoubi, Munir Ahmad, Syed Sheryar Akbar, Barween Al Kurdi, and Iman A. Akour. 2021. IoT for smart cities: Machine learning approaches in smart healthcare–A review. *Future Internet* 13, 8 (2021), 218.

Nabil Hachem, Yosra Ben Mustapha, Gustavo Gonzalez Granadillo, and Herve Debar. 2011. Botnets: Lifecycle and taxonomy. In *Proceedings of the 2011 Conference on Network and Information Systems Security*. 1–8. https://doi.org/10.1109/SAR-SSI.2011.5931395

Hamed HaddadPajouh, Ali Dehghantanha, Raouf Khayami, and Kim-Kwang Raymond Choo. 2018. A deep recurrent neural network based approach for Internet of Things malware threat hunting. *Future Generation Computer Systems* 85 (2018), 88–96.

Greg Hamler and Charles Elkan. 2004. Learning the k in k-means. *Advances in Neural Information Processing Systems* 16 (2004), 281–288.

Maaz Hasan. 2019. A Hybrid Real-Time Intrusion Detection System for an Internet of Things Environment with Signature and Anomaly Based Intrusion Detection. Master’s Thesis. National College of Ireland, Dublin. http://trap.ncirl.ie/4163/.

Mahmudul Hasan, Milan Islam, Ishrak Islam Zarif, and M. M. A. Hashem. 2019. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. *Internet of Things* 7 (Sept. 2019), 100059.

Mahmudul Hasan, Milan Islam, Ishrak Islam Zarif, and M. M. A. Hashem. 2019. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. *Internet of Things* 7 (Sept. 2019), 100059. https://doi.org/10.1016/j.iot.2019.100059

Geoffrey E. Hinton. 2009. Deep belief networks. *Scholarpedia* 4, 5 (2009), 5947.

SyedShehryarAkbar,BarweenAlKurdi,andImanA.Akour.2021.Iotforsmartcities:Machinelearningapproachesin smart healthcare—A review. *Future Internet* 13, 8 (2021), 218.

MehdiHosseinzadeh,AmirMasoudRahmani,BayYo,MoazamBidaki,MohammadMasdari,andMehranZangakani. 2021. Improving security using SVM-based anomaly detection: Issues and challenges. *Soft Computing* 25, 4 (2021), 3195–3223.

Philokypros Ioulianou, Vasileios Vasilakis, Ioannis Moscholios, and Michael Logothetis. 2018. A signature-based intrusion detection system for the Internet of Things. In *Proceedings of the Information and Communication Technology Forum*. 2019.

Atreyi Kankanhalli, Yannis Charalabidis, and Sehl Mellouli. 2019. IoT and AI for smart government: A research agenda. *Computers & Electrical Engineering* 79 (Oct. 2019), 106460. https://doi.org/10.1016/j.compeleceng.2019.106460
[78] Kenneth Kimani, Vitalice Oduol, and Kibet Langat. 2019. Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection* 25 (2019), 36–49.

[79] Maria Kjaerland. 2006. A taxonomy and comparison of computer security incidents from the commercial and government sectors. *Computers & Security* 25, 7 (Oct. 2006), 522–538. https://doi.org/10.1016/j.cose.2006.08.004

[80] Nickolaos Koroniotis, Mour Moustafà, Elena Sittikova, and Benjamin Turnbull. 2019. Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-iot dataset. *Future Generation Computer Systems* 100 (2019), 779–796. https://doi.org/10.1016/j.future.2019.05.041

[81] Prabhat Kumar, Govind P. Gupta, and Rakesh Tripathi. 2021. A distributed ensemble design based intrusion detection system using fog computing to protect the Internet of Things networks. *Journal of Ambient Intelligence and Humanized Computing* 12, 10 (2021), 9555–9572.

[82] Badr Lahasnand Hussein Samma. 2022. Optimized deep autoencoder model for Internet of Things intruder detection. *IEEE Access* 10 (2022), 8434–8448.

[83] Wenzhao Li, Weizhi Meng, and Man Ho Au. 2020. Enhancing collaborative intrusion detection via disagreement-based semi-supervised learning in IoT environments. *Journal of Network and Computer Applications* 161 (2020), 102631.

[84] Chih-Ta Lin, Sung-Lin Wu, and Mei-Lin Lee. 2017. Cyber attack and defense on industry control systems. In *Proceedings of the 2017 IEEE Conference on Dependable and Secure Computing*, 524–526. https://doi.org/10.1109/DESEC.2017.8073874

[85] Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao. 2017. A survey on Internet of Things: Architectures, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal* 4, 5 (2017), 1125–1142.

[86] Min Lin, Qiang Chen, and Shuicheng Yan. 2013. Network in network. *arXiv preprint arXiv:1312.4400* (2013).

[87] Zhen Ling, Junzhou Luo, Yiling Xu, Chao Gao, Kui Wu, and Xinwen Fu. 2017. Security vulnerabilities of Internet of Things: A case study of the smart plug system. *IEEE Internet of Things Journal* 4, 6 (2017), 1899–1909.

[88] Chang Liu, Chi Yang, Xuyun Zhang, and Jinjun Chen. 2015. External integrity verification for outsourced big data in cloud and IoT: A big picture. *Future Generation Computer Systems* 49 (2015), 58–67.

[89] Jun Liu, Jingpan Bai, Huahua Li, and Bo Sun. 2022. Improved LSTM-based abnormal stream data detection and correction system for Internet of Things. *IEEE Transactions on Industrial Informatics* 18, 2 (2022), 1282–1290. https://doi.org/10.1109/TII.2021.3079504

[90] Jinxin Liu, Michele Nogueira, Johan Fernandes, and Burak Kantarci. 2022. Adversarial machine learning: A multilayer review of the state-of-the-art and challenges for wireless and mobile systems. *IEEE Communications Surveys Tutorials* 24, 1 (2022), 123–159. https://doi.org/10.1109/COMST.2021.3136132

[91] Jing Liu, Yang Xiao, and C. L. Philip Chen. 2012. Authentication and access control in the Internet of Things. In *Proceedings of the 2012 32nd International Conference on Distributed Computing Systems Workshops*. IEEE, Los Alamitos, CA, 588–592.

[92] Qi Liu, Veit Hagenmeyer, and Hubert B. Keller. 2021. A review of rule learning-based intrusion detection systems and their prospects in smart grids. *IEEE Access* 9 (2021), 57542–57564.

[93] Xiaolong Liu, Yuxin Liu, Anfeng Liu, and Laurence T. Yang. 2018. Defending ON–OFF attacks using light probing messages in smart sensors for industrial communication systems. *IEEE Transactions on Industrial Informatics* 14, 9 (2018), 3801–3811.

[94] Yuxin Liu, Ming Ma, Xiao Liu, Neal N. Xiong, Anfeng Liu, and Ying Zhu. 2018. Design and analysis of probing route to defense sink-hole attacks for Internet of Things security. *IEEE Transactions on Network Science and Engineering* 7, 1 (2018), 356–372.

[95] Xinxin Lou and Asmaa Tellabi. 2020. Cybersecurity threats, vulnerability and analysis in safety critical industrial control system (ICS). In *Recent Developments on Industrial Control Systems Resilience*, Emil Pricop, Jaouhar Fattahi, Nithul Dutta, and Mariam Ibrahim (Eds.). Springer International Publishing, Cham, Switzerland, 75–97. https://doi.org/10.1007/978-3-030-31328-9

[96] Zhihan Lv, Liang Qiao, Jinhua Li, and Houbing Song. 2020. Deep-learning-enabled security issues in the Internet of Things. *IEEE Internet of Things Journal* 8, 12 (2020), 9531–9538.

[97] Chen Lyu, Xiaomei Zhang, Zhiqiang Liu, and Chi-Hung Chi. 2019. Selective authentication based geographic opportunistic routing in wireless sensor networks for Internet of Things against DoS attacks. *IEEE Access* 7 (2019), 31068–31082.

[98] Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, and Imran Zualkernan. 2015. Internet of Things (IoT) security: Current status, challenges and prospective measures. In *Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST'15)*. IEEE, Los Alamitos, CA, 336–341.

[99] Ritesh K. Malaiya, Donghwoon Kwon, Sang C. Suh, Hyunjoo Kim, Ikkyun Kim, and Jinoh Kim. 2019. An empirical evaluation of deep learning for network anomaly detection. *IEEE Access* 7 (2019), 140806–140817. https://doi.org/10.1109/ACCESS.2019.2943249

ACM Computing Surveys, Vol. 55, No. 5, Article 105. Publication date: December 2022.
[100] Jatinder Manhas and Shalu Kotwal. 2021. Implementation of intrusion detection system for Internet of Things using machine learning techniques. In Multimedia Security. Springer, 217–237.

[101] Mirco Marchetti, Fabio Pierazz, Michele Colajanni, and Alessandro Guido. 2016. Analysis of high volumes of network traffic for advanced persistent threat detection. Computer Networks 109 (2016), 127–141.

[102] James McCarthy, Lauren Aciero, Glen Joy, Jason Kuruvilla, Titilayo Ogunyale, Nikolas Urlaub, John Wiltberger, and Devin Wynne. 2020. Energy Sector Asset Management: For Electric Utilities, Oil & Gas Industry. Special Publication (NIST SP): 1800-23. NIST.

[103] Jason M. McGimthy and Alan J. Michaels. 2019. Secure industrial Internet of Things critical infrastructure node design. IEEE Internet of Things Journal 6, 5 (2019), 8021–8037.

[104] Yair Meidan, Michael Bohdana, Yael Mathov, Yisroel Mirsky, Dominik Breitenbacher, Asaf Shbatai, and Yuval Elovici. 2018. N-Balot: Network-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervasive Computing 17, 3 (July 2018), 12–22. doi:10.1109/MPRV.2018.03367731

[105] Douglas C. Montgomery, Elizabeth A. Peck, and Geoffrey Vining. 2012. Introduction to Linear Regression Analysis. Vol. 821. John Wiley & Sons.

[106] Muhammad Arif Mughal, Xiong Luo, Ata Ullah, Subhan Ullah, and Zahid Mahmood. 2018. A lightweight digital signature based security scheme for human-centered Internet of Things. IEEE Access 6 (2018), 31630–31643. https://doi.org/10.1109/ACCESS.2018.2844406

[107] Geoff Mulligan. 2007. The 6LoWPAN architecture. In Proceedings of the 4th Workshop on Embedded Networked Sensors. 78–82.

[108] K. Nar and S. S. Sastry. 2018. An analytical framework to address the data exfiltration of advanced persistent threats. In Proceedings of the 2018 IEEE Conference on Decision and Control (CDC’18). 867–873. doi:10.1109/CDC.2018.8619834

[109] Tri Gia Nguyen, Trung V. Phan, Binh T. Nguyen, Chakchai So-In, Zubair Ahmed Baig, and SuraSak Sanguanpong. 2019. Search: A collaborative and intelligent NIDS architecture for SDN-based cloud IoT networks. IEEE Access 7 (2019), 107678–107694. https://doi.org/10.1109/ACCESS.2019.2932438

[110] M. Nicho and C. D. McDermott. 2019. Dimensions of ‘Yoicio’ vulnerabilities of advanced persistent threats. In Proceedings of the 2019 International Conference on Software, Telecommunications, and Computer Networks (SoftCOM’19). 1–5. https://doi.org/10.23919/SOFTCOM.2019.8903788

[111] J. Nivethan and M. Papa. 2016. On the use of open-source firewalls in ICS/SCADA systems. Information Security Journal: A Global Perspective 25, 1-3 (April 2016), 83–93. https://doi.org/10.1080/19393555.2016.1172283

[112] Sven Nõmm, Alejandro Guerra-Manzanares, and Hayretdin Bahsi. 2019. Towards the integration of a post-hoc interpretation step into the machine learning workflow for IoT botnet detection. In Proceedings of the 2019 18th IEEE International Conference on Machine Learning and Applications (ICMLA’19). 1162–1169. https://doi.org/10.1007/ICMLA.2019.00193

[113] Doohwan Oh, Deokho Kim, and Won Woo Ro. 2014. A malicious pattern detection engine for embedded security systems in the Internet of Things. Sensors 14, 12 (2014), 24188–24211.

[114] Salome Oniani, Gonçalo Marques, Sophio Barnovi, Ivan Miguel Pires, and Akash Kumar Bhoi. 2021. Artificial intelligence for Internet of Things and enhanced medical systems. In Bio-Inspired Neurocomputing. Springer, 43–59.

[115] ISO. n.d. Publicly Available Standards: ISO.

[116] F. X. Aubet and M. O. Pahl. 2018. DS2OS Traffic Traces. Retrieved April 23, 2022 from https://www.kaggle.com/francoisxa/ds2ostraffictraces.

[117] Spyridon Papastergiou, Haralambo Mouratidis, and Eleni-Maria Kalogeraki. 2021. Handling of advanced persistent threats and complex incidents in healthcare, transportation and energy ICT infrastructures. Evolving Systems 12 (2021), 91–108. doi:10.1007/s12530-020-09335-4

[118] Seong-Taek Park, Guozhong Li, and Jae-Chang Hong. 2020. A study on smart factory-based ambient intelligence context-aware intrusion detection system using machine learning. Journal of Ambient Intelligence and Humanized Computing 11, 4 (2020), 1405–1412. https://doi.org/10.1007/s12652-018-0998-6

[119] Segun I. Popoola, Bamidele Adebiyi, Mohammad Hammoudah, Haris Gacanin, and Guan Gui. 2021. Stacked recurrent neural network for botnet detection in smart homes. Computers & Electrical Engineering 92 (2021), 107039.

[120] Philipp Probst, Marvin N. Wright, and Anne-Laure Boulesteix. 2019. Hyperparameters and tuning strategies for random forest. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery 9, 3 (2019), e1301.

[121] Santiago Quintero-Bonilla and Angel Martín del Rey. 2020. A new proposal on the advanced persistent threat: A survey. Applied Sciences 10, 11 (2020), 3874. https://doi.org/10.3390/app10113874

[122] Aqsa Saeed Qureshi, Asifullah Khan, Nauman Shamim, and Muhammad Hanif Durad. 2020. Intrusion detection using deep sparse auto-encoder and self-taught learning. Neural Computing and Applications 32, 8 (2020), 3135–3147. doi:10.1007/s00521-019-04152-6
[123] Salman Rachmadi, Satria Mandala, and Dita Oktaria. 2021. Detection of DoS attack using AdaBoost algorithm on IoT system. In Proceedings of the 2021 International Conference on Data Science and Its Applications (ICoDSA’21). IEEE, Los Alamitos, CA, 28–33.

[124] P. Radianiev, D. De Roure, S. Cannady, R. M. Montalvo, R. Niculescu, and M. Huth. 2018. Economic impact of IoT cyber risk—Analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance. In Living in the Internet of Things: Cybersecurity of the—2018. Institution of Engineering and Technology, 1–9. https://doi.org/10.1049/cp.2018.0003

[125] Risto Rajala and Mika Westerlund. 2007. Business models—A new perspective on firms’ assets and capabilities: Observations from the Finnish software industry. International Journal of Entrepreneurship and Innovation 8, 2 (2007), 115–125.

[126] Mamata Rath, Jyotirmaya Satpathy, and George S. Oreku. 2021. Artificial intelligence and machine learning applications in cloud computing and Internet of Things. In Artificial Intelligence to Solve Pervasive Internet of Things Issues. Elsevier, 103–123.

[127] Ravi Vinayakumar, Mamoun Alazab, Sriram Srinivasan, Ajay Arunachalam, and K. P. Soman. 2021. Adversarial defense: DGA-based botnets and DNS homographs detection through integrated deep learning. IEEE Transactions on Engineering Management. Early access, March 12, 2021.

[128] Abdul Razzaq, Khalid Latif, H. Farooq Ahmad, Ali Hur, Zahid Anwar, and Peter Charles Bloodsworth. 2014. Semantic security against web application attacks. Information Sciences 254 (Jan. 2014), 19–38. https://doi.org/10.1016/j.ins.2013.08.007

[129] Frederick J. Riggins and Samuel Fosso Wamba. 2015. Research directions on the adoption, usage, and impact of the Internet of Things through the use of big data analytics. In Proceedings of the 2015 48th Hawaii International Conference on System Sciences. 1531–1540. https://doi.org/10.1109/HICSS.2015.186

[130] Jose Roldán, Juan Boubeta-Puig, José Luis Martínez, and Guadalupe Ortiz. 2020. Integrating complex event processing and machine learning: An intelligent architecture for detecting IoT security attacks. Expert Systems with Applications 149 (July 2020), 113251. https://doi.org/10.1016/j.eswa.2020.113251

[131] Rodrigo Roman, Pablo Najera, and Javier Lopez. 2011. Securing the Internet of Things. Computer 44, 9 (2011), 51–58.

[132] Imed Romdhani. 2017. Confidentiality and security for IoT based healthcare. In Securing the Internet of Things. Elsevier, 133–139.

[133] Ahmad-Reza Sadeghi, Christian Wachsmann, and Michael Waidner. 2015. Security and privacy challenges in Industrial Internet of Things. In Proceedings of the 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC’15). IEEE, Los Alamitos, CA, 1–6.

[134] S. Rasoul Safavian and David Landgrebe. 1991. A survey of decision tree classifier methodology. IEEE Transactions on Systems, Man, and Cybernetics 21, 3 (1991), 660–674.

[135] Alan Saied, Richard E. Overill, and Tomasz Radzik. 2016. Detection of known and unknown DDoS attacks using artificial neural networks. Neurocomputing 172 (Jan. 2016), 385–393. https://doi.org/10.1016/j.neucom.2015.04.101

[136] Iqbal H. Sarker, Yoosuf B. Abushark, Fawaz Alsolami, and Asif Irshad Khan. 2020. IntruDTree: A machine learning based cyber security intrusion detection model. Symmetry 12, 5 (2020), 754.

[137] Robert E. Schapire. 2013. Explaining AdaBoost. In Empirical Inference. Springer, 37–52.

[138] Erich Schubert, Jörg Sander, Martin Ester, Hans Peter Kriegel, and Xiaowei Xu. 2017. DBSCAN revisited, revisited: Why and how you should (still) use DBSCAN. ACM Transactions on Database Systems 42, 3 (July 2017), Article 19, 21 pages. https://doi.org/10.1145/3068335

[139] Sebastian Garcia, Agustin Parmisano, and Maria Jose Enquigao. 2020. IoT-23: A labeled dataset with malicious and benign IoT network traffic (Version 1.0.0) [Data set]. Zenodo. http://doi.org/10.5281/zenodo.4743746

[140] Ludwig Seitz, Göran Selander, and Christian Gehrmann. 2013. Authorization framework for the Internet-of-Things. In Proceedings of the 2013 IEEE 14th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM’13). IEEE, Los Alamitos, CA, 1–6.

[141] Jayasree Sengupta, Sushmita Ruj, and Sipra Das Bit. 2020. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IoT. Journal of Network and Computer Applications 149 (2020), 102481.

[142] Muhammad Shafiq, Zhihong Tian, Yanbin Sun, Xiaojiang Du, and Mohsen Guizani. 2020. Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for Internet of Things in smart city. Future Generation Computer Systems 107 (June 2020), 433–442. https://doi.org/10.1016/j.future.2020.02.017

[143] Muhammad Shafiq, Zhihong Tian, Yanbin Sun, Xiaojiang Du, and Mohsen Guizani. 2020. Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for Internet of Things in smart city. Future Generation Computer Systems 107 (June 2020), 433–442.

[144] Nataliya Shevchenko, Timothy A. Chick, Paige O’Riordan, Thomas Patrick Scanlon, and Carol Woody. 2018. Threat Modeling: A Summary of Available Methods. White Paper. Software Engineering Institute.
[145] Prachi Shukla. 2017. ML-IDS: A machine learning approach to detect wormhole attacks in Internet of Things. In Proceedings of the 2017 Intelligent Systems Conference (IntelliSys’17). IEEE, Los Alamitos, CA, 234–240.

[146] Daniel L. Silver, Qiang Yang, and Lianghao Li. 2013. Lifelong machine learning systems: Beyond learning algorithms. In Proceedings of the 2013 AAAI Spring Symposium Series.

[147] Pradeep Singh and M. Venkatesan. 2018. Hybrid approach for intrusion detection system. In Proceedings of the 2018 International Conference on Current Trends Towards Converging Technologies (ICTCT’18). IEEE, Los Alamitos, CA, 1–5.

[148] Emiliano Sisinni, Abusayeed Saifullah, Song Han, Ulf Jernelov, and Mikael Gidlund. 2018. Industrial Internet of Things: Challenges, opportunities, and directions. IEEE Transactions on Industrial Informatics 14, 11 (2018), 4724–4734.

[149] Richard E. Smith. 2001. Authentication: from Passwords to Public Keys. Addison Wesley Longman.

[150] S. Sriram, K. Simran, R. Vinayakumar, S. Akash, and K. P. Soman. 2020. Towards evaluating the robustness of deep intrusion detection models in adversarial environment. In Security and Computing in Communications, Sabu M. Thampi, Gregorio Martinez Perez, Ryan Ko, and Danda B. Rawat (Eds.). Communications in Computer and Information Science. Springer, Singapore, 111–120. https://doi.org/10.1007/978-981-15-4825-3

[151] S. Sriram, R. Vinayakumar, Mamoun Alazab, and K. P. Soman. 2020. Network flow based IoT botnet attack detection using deep learning. In Proceedings of the 2020 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS’20). IEEE, Los Alamitos, CA, 189–194.

[152] S. Sriram, R. Vinayakumar, V. Sowmya, Mamoun Alazab, and K. P. Soman. 2020. Multi-scale learning based malware variant detection using spatial pyramid pooling network. In Proceedings of the 2020 Conference on Computer Communications Workshops (INFOCOM WKSHPS’20), 740–745. https://doi.org/10.1109/INFOCOMWKSHPS50652.2020.9162661

[153] Nasrin Sultana, Naveen Chilamkurti, Wei Peng, and Rabie Alhadad. 2019. Survey on SDN based network intrusion detection system using machine learning approaches. Peer-to-Peer Networking and Applications 12, 2 (March 2019), 493–501. https://doi.org/10.1007/s12083-017-0630-0

[154] Colin Tankard. 2011. Advanced persistent threats and how to monitor and deter them. Network Security 2011, 8 (2011), 16–19. https://doi.org/10.1016/S1353-4858(11)70086-1

[155] Colin Tankard. 2011. Advanced persistent threats and how to monitor and deter them. Network Security 2011, 8 (2011), 16–19.

[156] Mahbod Tavallaeae, Natalia Stakhanova, and Ali Akbar Ghorbani. 2010. Toward credible evaluation of anomaly-based intrusion-detection methods. IEEE Transactions on Systems, Man, and Cybernetics: Part C (Applications and Reviews) 40, 5 (2010), 516–524.

[157] Evangelos Theodoridis, Georgios Mylonas, and Ioannis Chatzigiannakis. 2013. Developing an IoT smart city framework. In Proceedings of the International Conference on Information, Intelligence, Systems, and Applications (IISA’13). IEEE, Los Alamitos, CA, 1–6.

[158] Zhihong Tian, Wei Shi, Yuhang Wang, Chunsheng Zhu, Xiaojiang Du, Shun Su, Yanbin Sun, and Nadra Guizani. 2019. Real-time lateral movement detection based on evidence reasoning network for edge computing environment. IEEE Transactions on Industrial Informatics 15, 7 (2019), 4285–4294.

[159] Y. P. Tsang, C. H. Wu, W. H. Ip, and Wen-Lung Shiau. 2021. Exploring the intellectual cores of the blockchain–Internet of Things (BioT). Journal of Enterprise Information Management 34, 5 (2021), 1287–1317.

[160] Anton V. Uzunov and Eduardo B. Fernandez. 2014. An extensible pattern-based library and taxonomy of security threats for distributed systems. Computer Standards & Interfaces 36, 4 (June 2014), 734–747. https://doi.org/10.1016/j.csi.2013.12.008

[161] Michael Vai, Ben Nahill, Josh Kramer, Michael Geis, Dan Utin, David Whelihan, and Roger Khazan. 2015. Secure architecture for embedded systems. In Proceedings of the 2015 IEEE High Performance Extreme Computing Conference (HPEC’15). IEEE, Los Alamitos, CA, 1–5.

[162] Emmanouil Vasilomanolakis, Shankar Karuppayah, Max Mühlhäuser, and Mathias Fischer. 2015. Taxonomy and survey of collaborative intrusion detection. ACM Computing Surveys 47, 4 (2015), 1–33.

[163] S. Venkatraman and B. Surendiran. 2020. Adaptive hybrid intrusion detection system for crowd sourced multimedia Internet of Things. Systems. Multimedia Tools and Applications 79, 5 (2020), 3993–4010.

[164] Abhishek Verma and Virender Ranga. 2019. Evaluation of network intrusion detection systems for RPL based 6LoWPAN networks in IoT. Wireless Personal Communications 108, 3 (2019), 1571–1594. https://doi.org/10.1007/s11277-019-06485-w

[165] Abhishek Verma and Virender Ranga. 2020. Machine learning based intrusion detection systems for IoT applications. Wireless Personal Communications 111, 4 (2020), 2287–2310. https://doi.org/10.1007/s11277-019-06986-8

[166] R. Vinayakumar, Mamoun Alazab, K. P. Soman, Prabaharan Poornachandran, Ameer Al-Nemrat, and Sitalakshmi Venkatraman. 2019. Deep learning approach for intelligent intrusion detection system. IEEE Access 7 (2019), 41525–41550. https://doi.org/10.1109/ACCESS.2019.2895334
[167] R. Vinayakumar, Mamoun Alazab, Sriram Srinivasan, Quoc-Viet Pham, Soman Koti Padannayil, and K. Simran. 2020. A visualized botnet detection system based deep learning for the Internet of Things networks of smart cities. *IEEE Transactions on Industry Applications* 56, 4 (2020), 4436–4456.

[168] R. Vinayakumar, K. P. Soman, Prabaharan Poornachandran, Mamoun Alazab, and Alireza Jolfaei. 2019. DBD: Deep learning DGA-based botnet detection. In *Deep Learning Applications for Cyber Security*. Springer. 127–149.

[169] David Wagner and R. Dean. 2001. Intrusion detection via static analysis. In *Proceedings of the 2001 IEEE Symposium on Security and Privacy (S&P’01)*. IEEE, Los Alamitos, CA, 156–168.

[170] Arfan Haider Wahla, Lan Chen, Yali Wang, Rong Chen, and Fan Wu. 2019. Automatic wireless signal classification in multimedia Internet of Things: An adaptive boosting enabled approach. *IEEE Access* 7 (2019), 160334–160344.

[171] Tian Wang, Zakirul Alam Bhuiyan, Guojun Wang, Liangyong Qi, Jie Wu, and Thaier Hayajneh. 2019. Preserving balance between privacy and data integrity in edge-assisted Internet of Things. *IEEE Internet of Things Journal* 7, 4 (2019), 2679–2689.

[172] Xiali Wang and Xiang Lu. 2020. A host-based anomaly detection framework using XGBoost and LSTM for IoT devices. *Wireless Communications and Mobile Computing* 2020 (2020), 1–13.

[173] Muhammad Waqas, Kamlesh Kumar, Asif Ali Laghari, Umar Saeed, Muhammad Malook Rind, Aftab Ahmed Shaikh, Fahad Hussain, Athaul Rai, and Abdul Qayoom Qazi. 2021. Botnet attack detection in Internet of Things devices over cloud environment via machine learning. *Concurrency and Computation: Practice and Experience* 2021 (2021), e6662.

[174] Michael Weiner, Wolfgang Wieser, Emili Lupon, Georg Sigl, and Salvador Manich. 2019. A calibratable detector for invasive attacks. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 27, 5 (2019), 1067–1079.

[175] Peter Weiß, Bernhard Koelmel, and Rebecca Bulander. 2016. Digital service innovation and smart technologies: Developing digital strategies based on Industry 4.0 and product service systems for the renewal energy sector. In *Proceedings of the 26th Annual RESER Conference*.

[176] Christian Wressnegger, Guido Schwenk, Daniel Arp, and Konrad Rieck. 2013. A close look on n-grams in intrusion detection: Anomaly detection vs. classification. In *Proceedings of the 2013 ACM Workshop on Artificial Intelligence and Security*. 67–76.

[177] Hansong Xu, Wei Yu, David Griffith, and Nada Golmie. 2018. A survey on industrial Internet of Things: A cyber-physical systems perspective. *IEEE Access* 6 (2018), 78238–78259.

[178] Yikai Xu, Yi Yang, Tianran Li, Jiaqi Ju, and Qi Wang. 2017. Review on cyber vulnerabilities of communication protocols in industrial control systems. In *Proceedings of the 2017 IEEE Conference on Energy Internet and Energy System Integration* (EI2’17). 1–6. https://doi.org/10.1109/EI2.2017.8245509

[179] Kun Yang, Samory Kpotufe, and Nick Feamster. 2021. An efficient one-class SVM for anomaly detection in the Internet of Things. *arXiv preprint arXiv:2104.11146* (2021).

[180] Ning Ye, Yan Zhu, Ru-Chuan Wang, Reza Malekian, and Qiao-Min Lin. 2014. An efficient authentication and access control scheme for perception layer of Internet of Things. *Applied Mathematics and Information Sciences* 8, 4 (2014), 1617–1624.

[181] Wojciech Zaremba, Iryna Sutskever, and Oriol Vinyals. 2014. Recurrent neural network regularization. *arXiv preprint arXiv:1409.2329* (2014).

[182] Bruno Bogaz Zarpelão, Rodrigo Sanches Miani, Cláudio Toshio Kawakami, and Sean Carlisto de Alvarena. 2017. A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications* 84 (2017), 25–37.

[183] Chongzhen Zhang, Yanli Chen, Yang Meng, Fangming Ruan, Runze Chen, Yidan Li, and Yaru Yang. 2021. A novel framework design of network intrusion detection based on machine learning techniques. *Security and Communication Networks* 2021 (2021), Article 661075.

[184] Hao Zhang, Yongdan Li, Zhihan Lv, Arun Kumar Sangaiah, and Tao Huang. 2020. A real-time and ubiquitous network attack detection based on deep belief network and support vector machine. *IEEE/CAA Journal of Automatica Sinica* 7, 3 (2020), 790–799.

[185] Ying Zhang, Peisong Li, and Xinheng Wang. 2019. Intrusion detection for IoT based on improved genetic algorithm and deep belief network. *IEEE Access* 7 (2019), 31711–31722.

[186] Kai Zhao and Lina Ge. 2013. A survey on the Internet of Things security. In *Proceedings of the 2013 9th International Conference on Computational Intelligence and Security*. IEEE, Los Alamitos, CA, 663–667.

[187] Aaron Zimba, Hongsong Chen, Zhaoshun Wang, and Mumbi Chishimba. 2020. Modeling and detection of the multistages of advanced persistent threats attacks based on semi-supervised learning and complex networks characteristics. *Future Generation Computer Systems* 106 (2020), 501–517. https://doi.org/10.1016/j.future.2020.01.032

[188] Thi Thi Zin, Pyke Tin, and Hiromitsu Hama. 2016. Reliability and availability measures for Internet of Things consumer world perspectives. In *Proceedings of the 2016 IEEE 5th Global Conference on Consumer Electronics*. IEEE, Los Alamitos, CA, 1–2.
[189] Iveta Zolotová, Marek Bundzel, and Tomáš Lojka. 2015. Industry IoT gateway for cloud connectivity. In Advances in Production Management Systems: Innovative Production Management Towards Sustainable Growth, Shigeki Umeda, Masaru Nakano, Hajime Mizuyama, Hironori Hibino, Dimitris Kiritsis, and Gregor von Cieminski (Eds.). IFIP Advances in Information and Communication Technology. Springer International Publishing, Cham, Switzerland, 59–66. https://doi.org/10.1007/978-3-319-22759-7_7

Received 27 April 2021; revised 22 March 2022; accepted 6 April 2022