*mathematics*

MDPI

*Review*

# Advanced Persistent Threats and Their Defense Methods in Industrial Internet of Things: A Survey

**Chenquan Gan [1,2,*], Jiabin Lin [1], Da-Wen Huang [3], Qingyi Zhu [2] and Liang Tian [4]**

[1] School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China; s210101083@stu.cqupt.edu.cn
[2] School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing 400065, China; zhuqy@cqupt.edu.cn
[3] College of Computer Science, Sichuan Normal University, Chengdu 610101, China; hdawen1@gmail.com
[4] School of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China; besttianliang@gmail.com
* Correspondence: gcq2010cqu@163.com

**Abstract:** The industrial internet of things (IIoT) is a key pillar of the intelligent society, integrating traditional industry with modern information technology to improve production efficiency and quality. However, the IIoT also faces serious challenges from advanced persistent threats (APTs), a stealthy and persistent method of attack that can cause enormous losses and damages. In this paper, we give the definition and development of APTs. Furthermore, we examine the types of APT attacks that each layer of the four-layer IIoT reference architecture may face and review existing defense techniques. Next, we use several models to model and analyze APT activities in IIoT to identify their inherent characteristics and patterns. Finally, based on a thorough discussion of IIoT security issues, we propose some open research topics and directions.

**Keywords:** industrial internet of things; advanced persistent threat; security analysis; modeling analysis

**MSC:** 49N90

check for updates

**Citation:** Gan, C.; Lin, J.; Huang, D.-W.; Zhu, Q.; Tian, L. Advanced Persistent Threats and Their Defense Methods in Industrial Internet of Things: A Survey. *Mathematics* **2023**, *11*, 3115. https://doi.org/10.3390/math11143115

Academic Editor: Daniel-Ioan Curiac

Received: 12 June 2023
Revised: 4 July 2023
Accepted: 12 July 2023
Published: 14 July 2023

**Copyright:** © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

## 1. Introduction

The industrial internet of things (IIoT) refers to the application of internet of things (IoT) technology in the industrial field, achieving intelligent interconnection and data exchange by connecting various sensors, equipment, and networks [1]. IIoT aims to achieve digital transformation, increase production efficiency, reduce costs, improve product quality, and coordinate supply chains, with applications spanning fields such as manufacturing, energy, utilities, and transportation [2,3].

With the development of technology, IIoT is widely used in the field of industrial automation and intelligence, which helps to improve the efficiency and quality of industrial production. At the same time, IIoT is vulnerable to advanced persistent threat (APT) attacks due to its evolving technological paradigm [4]. The increasing interconnectivity of industrial infrastructure equipment has expanded the attack surface, making it a prime target for network attacks [5]. The threats facing the IIoT can not only cause enormous property damage but also threaten human life and safety [6]. APTs refer to the behavior of highly specialized hackers or cybercriminal organizations that use targeted, hard-to-detect, and long-lasting attack methods to attack a specific target [7]. Compared to traditional attacks, APTs are not used to disrupt services but mainly to steal intellectual property, sensitive internal business, legal documents, and other data [8].

We summarize the reasons why IIoT is vulnerable to APT attacks as follows:

- Complexity [9]: IIoT networks usually consist of equipment and systems, including sensors, controllers, gateways, and cloud services. The complexity of these types of equipment and these systems make them vulnerable to attacks, and attackers can hide and spread within them.
- Centralized control [10]: IIoT networks are usually managed by one or more central control systems, which can be invaded and controlled by attackers, thus gaining control over the entire network.
- Insecure design [11]: Many types of IIoT equipment and many IIoT systems are designed for ease of use, without sufficient consideration for security. For example, some types of equipment may use default usernames and passwords, making them vulnerable to password-based attacks.
- Lack of updates and patches [12]: Many types of IIoT equipment and systems run for long periods without updates and patches, making them vulnerable to attacks exploiting known vulnerabilities.
- Data sensitivity [13]: Data in IIoT networks are often sensitive, and attackers can use these data for espionage, ransomware, and other malicious activities.

From an attack point of view, IIoT often involves more complex network architectures [4,5] and usually involves higher security risks [6]. Through these works [4–6,9–13], we compare IoT and IIoT in Table 1.

**Table 1.** Comparison between IoT and IIoT.

| Feature | IoT | IIoT |
|---|---|---|
| Definition | Internet system connecting equipment and networks | Internet of things system applied in industrial field |
| Application area | Family, medical care, agriculture, urban management, and transportation | Factory automation, equipment monitoring, quality control, and logistics management |
| Equipment types | Smartphones, watches, and home appliances | Robots, sensors, and PLC |
| Communication mode | Wireless network technology | Communication protocol |
| Data transmission | Large quantity, little influence on transmission speed | Little quantity, great influence on transmission speed |
| Usual network structure | Smart equipment and cloud services | Multiple types, multiple levels |
| Usual security risks | Personal information, behavioral habits | Key infrastructure, production safety, and personnel health |

In summary, IIoT provides great convenience for human production and life but also faces APT attacks. This review summarizes APTs and defense methods at each layer of the IIoT architecture and analyzes APT activities by establishing models.

### *1.1. Contributions*

When facing APTs in IIoT, Qi et al. [14] implemented network security policies and measures to directly prevent APTs. The work [15] identified APTs through detection technology to prevent attacks. Reference [16] provided various methods to protect IIoT equipment and data. For defending against APTs, there are specific measures in three directions.

(1) Strategies and measures including network isolation, access control, and encryption [14]. Network isolation refers to isolating IIoT from other networks to prevent APT attacks from spreading to IIoT [17]. This approach can reduce the scope of attacks, but it also reduces system flexibility and availability and requires more management and maintenance costs. Access control refers to authenticating users and equipment

and controlling their access to ensure system security [18,19]. This approach can provide some security guarantees, but it requires maintaining and managing a large amount of authentication information, increasing management costs. Encryption technology refers to using encryption technology to protect data transmission and storage [20]. This approach can provide a certain degree of security guarantee, but it may have a certain impact on system performance, and there is a risk of password cracking. However, these methods affect the smoothness and efficiency of production and industrial processes. Moreover, they cannot completely prevent APT attacks as attackers can use advanced techniques to bypass these measures.

(2) Detection technologies include network traffic monitoring-based, anomaly detection-based, attack graph-based, behavior analysis-based, and artificial intelligence-based methods [15]. The network traffic monitoring-based method detects and analyzes abnormal data flows and behaviors in the IIoT network by monitoring the network flow to identify possible APT attacks [21,22]. However, this method depends on the accuracy and efficiency of flow monitoring. If attackers adopt covert attack methods such as staged attacks and forged traffic, this method may not effectively detect attacks. The anomaly detection-based method models the behavior of IIoT system equipment and users and detects abnormal behavior to identify possible APT attacks [23]. This method requires sufficient data training and modeling and also needs to handle a large number of false positives and false negatives. It also needs to overcome the challenge of attackers adopting covert attacks. The attack graph-based method identifies possible APT attacks by analyzing the attacker's attack path and target on the IIoT system [24]. This method requires comprehensive security modeling and attack graph analysis of the IIoT system, but the components and connections in the IIoT system are often very complex. Therefore, the modeling and analysis work of this method requires a high human and time cost. The behavior analysis-based method analyzes the behavior of equipment, users, and networks and detects any abnormal behavior [25]. The behavior analysis-based method may have a higher false positive rate because normal behavior may be mistaken for abnormal behavior, thus increasing management and maintenance costs. Artificial intelligence uses machine learning and deep learning algorithms to monitor the behavior of IIoT systems and detect abnormal activities [26]. Machine learning and deep learning algorithms may generate false positives or false negatives, so the algorithms need to be continuously improved and trained. In conclusion, these detection methods require sufficient labeled data in industrial environments, which increases costs. In addition, attackers can use adversarial techniques to deceive detection methods, further increasing the difficulty of defending against APTs in IIoT.

(3) Using hardware security, firewalls, and vulnerability management for the security of IIoT equipment and data [16]. Hardware security refers to the use of hardware equipment and security chips to protect the security of IIoT [14,18]. This method can provide high security but is costly and also carries the risk of supply chain attacks and physical attacks. Firewalls refer to the use of firewalls between the IIoT system and external networks to limit access and traffic [27]. The disadvantage is that firewalls may not be able to prevent all attacks, such as APT attackers who may use disguised traffic or application-based attacks. Vulnerability management refers to the timely discovery and repair of vulnerabilities in the system to avoid APT attacks [28,29]. This method requires continuous vulnerability scanning and management and timely patching, but this may take a lot of time and effort, and attackers may find new vulnerabilities to attack the system.

Overall, there are many methods to prevent APT attacks in IIoT systems, but each method has its own limitations and flaws. Therefore, it is necessary to comprehensively apply these methods and continuously improve and optimize the security protection mechanisms of IIoT systems based on practical situations. To provide a more detailed description and analysis of the APT activities faced by IIoT, this paper proposes a series

of recommendations for the security of IIoT networks through a layered study of APTs in industrial IoT. Specifically, the main contributions of this paper are as follows:

(1) A comprehensive introduction to the definition and classification of APTs in industrial IoT. This survey lists the differences between APTs and traditional attacks from different dimensions and explores typical examples of APT attacks.
(2) A deep understanding of APTs in IIoT, and a layered study can help reveal the APT attacks faced by IIoT. This survey identifies potential weaknesses and vulnerabilities and APT attacks faced by each layer by analyzing attacks at different levels, such as the perception layer, transmission layer, platform layer, and application layer.
(3) Providing effective defense strategies for IIoT security. This survey provides multi-layer security defense mechanisms for IIoT security and helps propose security reinforcement strategies for APTs in IIoT through various models to characterize and analyze APT activities fundamentally.
(4) Outlook on the trends and research directions of APTs in future IIoT. This survey points out the current hotspots and challenges of APT research in IIoT, as well as possible solutions and development directions in the future, such as artificial intelligence and machine learning.

In a nutshell, this survey conducts a comprehensive and in-depth study of APTs in IIoT and proposes a series of feasible solutions and future research directions. These contributions will help improve the security of IIoT and ensure the stability and reliability of the production process.

### *1.2. Organization*

The remaining parts of this review are structured as follows. Section 2 gives the definition and development of APTs. Section 3 provides a detailed description of the APTs and defense mechanisms that each layer of IIoT architecture faces. Section 4 analyzes the models adopted when IIoT is faced with APTs. Section 5 performs a work comparison. Section 6 discusses some notable open research issues. Section 7 concludes the review.

## 2. Definition and Development of APTs

The definition of APTs is a new attack and security threat to a specific target by organizations (especially governments) or small groups using advanced attack methods. APTs are organized, targeted, covert, disruptive, and persistent. Unlike ordinary attacks or hacks, APTs are sophisticated, continuously latent, and difficult to track. Through works [7,8], the main characteristics of APTs are (1) well-targeted and harmful; (2) well-organised and well-resourced; (3) multiple attacks and continuous attacks; and (4) highly covert and difficult to trace. In Table 2, we compare traditional attacks and APTs in seven respects.

**Table 2.** Comparison between traditional attacks and APTs.

| Feature | Traditional Attacks | APTs |
|---|---|---|
| Attack mode | Viruses, worms, and ransomware | Social engineering, exploit, and backdoor attack |
| Purpose | Acquire property or destroy the system | Long-term access and control system |
| Discovery difficulty | Easily detected and intercepted | Difficult to detect and intercept |
| Attacker skill | Basic skills and tools | Advanced skills and tools |
| Defense strategy | Antivirus software, firewall, and encryption | Network monitoring, intrusion detection, and response system |
| Consequence | System interruption or data loss | Data leakage, financial loss, and reputation damage |

APTs have been studied for many years and pose a serious threat to IoT equipment [30]. APTs not only cause significant financial losses but also threaten human life safety [31]. The most significant feature of APTs is that they can evade high-level security systems, steal or manipulate information, and have a negative impact on equipment [32]. Stuxnet, an example of an APT, is a malicious virus that specifically targets industrial control systems. It disrupted the power generation plan of an Iranian nuclear power plant, delaying the program for four years [33]. The work [34] shows that Stuxnet infected over 45,000 industrial networks worldwide. Table 3 lists some famous APT attacks in recent years. Through these examples, we can draw the conclusion that APT is characterized by an extremely strong purpose; extremely advanced and complex attack methods, which were used before the vulnerability circle was made public; and finally attacks with a long attack time span, and hidden attacks.

**Table 3.** Attack cases of APTs in recent years.

| Name | Time (Year) | Target | Description |
|---|---|---|---|
| Industroyer [35] | 2016 | Ukrainian power grid | Power outages in some areas last for several hours |
| TRITON [36] | 2017 | Saudi oil factory | Destroy its safety control system |
| VPNFilter [37] | 2018 | The whole world | Infected router equipment |
| LockerGoga [38] | 2019 | Norwegian aluminum company | The factory was forced to shut down for several days |
| Winnti [39] | 2020 | Organizations in North America, Europe, and Asia | Stealing sensitive information and intellectual property rights |
| DarkSide [40] | 2021 | American Colonial Oil Pipeline Company | The oil pipeline was paralyzed for a week |

As a result, APTs have long durations and significant impacts. Studying the propagation patterns of APTs in IIoT and effective defense strategies against APTs in IIoT has become a critical and meaningful research topic for many scholars and companies. This is particularly crucial for preventing security issues in IIoT.

## 3. APTs Faced by IIoT and Its Defense Methods

In the previous section, we describe the definition and development of APTs. In this section, we describe the APTs faced by IIoT and ways to defend against them from the perspective of IIoT architecture. The IIoT architecture is a higher-level abstract description of IIoT that helps identify the problems and challenges in different application scenarios. The design of IIoT architecture needs to emphasize the scalability, modularity, interoperability, and scalability of heterogeneous equipment using different technologies. Several reference architecture frameworks originated from different application environments of IoT and IIoT in the past [41]. In reference to studies [42–45], this paper introduces a widely accepted 4-layer IIoT model as a reference architecture, as shown in Figure 1. This architecture includes the perception layer, transport layer, platform layer, and application layer according to different functions. The perception layer consists of various types of basic chips, sensors, RFID scanners, actuators, and other equipment. In an industrial environment, all this equipment may be accompanied by equipment such as conveyor systems and industrial robots. Equipment is responsible for capturing data and gathering

information. The transport layer can use Wi-Fi, Bluetooth, Nb-IoT, LoRa, etc., to transmit information to the processing system at the next layer. The platform layer is composed of a server and database, which is responsible for performing many tasks, such as making decisions, calculating optimization algorithms, and storing a large amount of data. Finally, the application layer is responsible for meeting the special needs of end users' applications. For example, intelligent factories and intelligent robots are considered to be applications of IIoT. Next, we will introduce these layers one by one, and the APTs and defense methods that may exist in each layer will be highlighted.

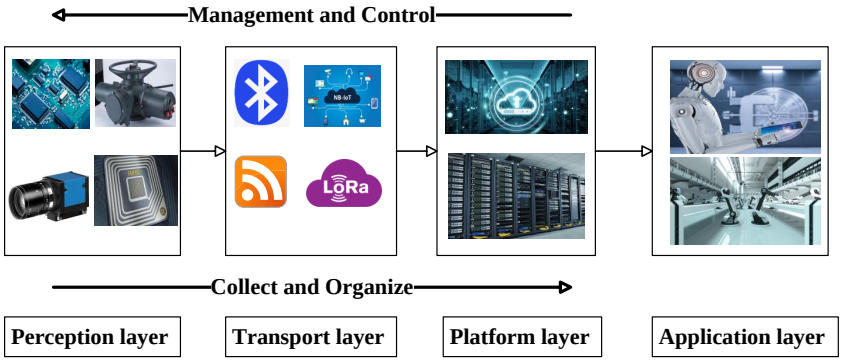


**Figure 1.** IIoT architecture.

### *3.1. Perception Layer*

The perception layer of IIoT, often referred to as the equipment layer, is composed of physical equipment such as industrial equipment and sensors that transmit data to the upper-level control system through the Internet [46,47]. APT attacks on the equipment layer may occur through malicious software or hardware intrusion, physical attacks, or equipment firmware vulnerabilities, among others, in order to gain control of equipment or steal equipment data.

- Physical attacks [48,49]: Attackers can physically attack equipment, for example, by disassembling it to obtain confidential information or by destroying it to paralyze factory production. This attack method requires attackers to have the opportunity to physically touch the equipment, but once successful, the consequences are usually severe;
- Human-based attacks [50]: Attackers can directly invade equipment or obtain access permissions through social engineering, among other methods. This attack method requires attackers to have certain technical capabilities and knowledge, but once successfully invaded, attackers can control the equipment for an extended period without being detected;
- Malware attacks [51,52]: Attackers can invade equipment by infecting them with malware and controlling them for the attack. This attack method is particularly dangerous because attackers can control equipment for a long time without being detected;
- Zero-day vulnerability exploitation [53,54]: Attackers can exploit unknown vulnerabilities to invade equipment and control them for the attack. This attack method is usually difficult to detect and prevent since the vulnerabilities have not yet been discovered.

In summary, the APTs that the IIoT perception layer faces are very serious, and comprehensive measures are needed to strengthen the security of equipment, such as using antivirus software, regularly updating system patches, and using network isolation. Additionally, regular security assessments and vulnerability scans are required, as well as raising employee awareness of security, and strengthening security training and education.

### *3.2. Transport Layer*

The transmission layer of IIoT, also known as the network layer, primarily provides ubiquitous connectivity for equipment and transmits generated data from the perception layer to the platform layer through a heterogeneous communication network aggregation [55,56]. In the transmission layer, APT attacks may include intrusion into gateways, eavesdropping or man-in-the-middle attacks on data transmission, and tampering with protocol conversion; the following are some common examples:

- Distributed denial-of-service (DDoS) attacks [57], where attackers can occupy IIoT network bandwidth and resources by sending a large number of requests, causing system crashes or becoming unusable;
- Phishing attacks [58], where attackers can send deceptive emails, messages, or other information to trick users into providing sensitive information or downloading malware;
- Malware attacks [51,52], where attackers can infect IIoT systems by sending malware or exploiting vulnerabilities, which may lead to confidential data leaks, system crashes, or other security issues;
- Wireless intrusion attacks [50], where attackers can invade IIoT systems by exploiting wireless network vulnerabilities. For example, they can use attacks against Wi-Fi or Bluetooth protocols to obtain sensitive information in the system.

To protect their IIoT networks against these threats, enterprises can take multiple measures such as strengthening network security monitoring, using secure authentication technologies, scanning and repairing system vulnerabilities, limiting network access, and using IoT equipment security protocols. Additionally, it is essential to train employees effectively on network security education and awareness.

### *3.3. Platform Layer*

The cloud platform layer is the core layer of the IIoT architecture, responsible for data storage, analysis, processing, and management. In the cloud platform layer, APT attacks may include intrusion into cloud servers, theft of cloud storage, and tampering with data analysis. The following are several aspects of these attacks.

- Physical layer attacks [48,49]: Attackers may use physical layer attack methods such as equipment intrusion and the interception of data streams to undermine the integrity and reliability of the IIoT platform. This type of attack can continue undetected and have a significant impact on the IIoT platform;
- Data leakage [59]: Due to the large amount of sensitive data that the IIoT platform needs to process, data leakage is a serious threat. Attackers may exploit weaknesses to steal sensitive information and use it for other attacks, such as identity theft and ransomware;
- Supply chain attacks [18,60]: Supply chain attacks involve attackers infiltrating the IIoT platform through third-party service providers or components in the platform's supply chain. This type of attack can last for a long time and cause significant damage to the platform without being detected.

To address these threats, companies should implement security measures on the IIoT platform, such as access control, authentication, encryption, vulnerability management, and security auditing. In addition, companies should maintain security patch updates, strengthen the monitoring of the IIoT platform, and provide effective cybersecurity training for employees.

### *3.4. Application Layer*

The application layer is the top layer of the IIoT architecture, which includes various applications and services, such as monitoring, control, diagnosis, and prediction. In the application layer, APT attacks may include intrusion into applications, tampering with application interfaces, and theft of user data, among others, as follows:

- Access control attacks [61]: Attackers may gain unauthorized access by stealing credentials, deceiving users, or exploiting vulnerabilities. Once attackers gain access, they can manipulate equipment, tamper with data, or steal sensitive information.

- Malware [51,52]: Attackers may infect equipment or networks with malware to control them. Malware may include viruses, worms, Trojans, or ransomware, which can damage equipment or entire systems.
- Denial-of-service attacks (DDoS) [57]: Attackers may launch DDoS attacks to make target equipment or make systems unavailable. This type of attack typically involves a large amount of traffic or a large number of requests that exceed the target system's processing capabilities, causing it to crash or become unusable.
- Physical attacks [48,49]: Attackers may invade equipment or systems physically, such as forcibly entering equipment or destroying physical connections. This type of attack can cause equipment or systems to stop working, lose data, or leak information.
- Social engineering attacks [50]: Attackers may use social engineering techniques to deceive users or administrators into disclosing credentials or performing inappropriate operations. This type of attack typically requires attackers to have some understanding of the target user's behavior patterns and psychological state.

To address these threats, the industrial internet application layer needs to take a series of security measures, including access control, encrypted communication, vulnerability management, behavioral analysis, and physical security, to ensure the security and reliability of equipment and systems.

### *3.5. Overall Architecture of IIoT*

A layered approach to researching IIoT can help deepen our understanding of the different levels and components of IIoT, refine the APT attack issues faced, improve systemic thinking, support innovation and application, and promote better protection of IIoT. However, the APT attacks faced by the entire IIoT system are very complex, and this article summarizes some means of defending against APT attacks.

- Strengthen the security of IIoT equipment [62,63], enhance access control and the authentication of equipment, use encryption technology to protect data transmission, regularly update firmware and software to fix known vulnerabilities, and restrict IoT equipment access to the network;
- Strengthen network security, use security equipment such as firewalls [64] and intrusion detection systems [65] to monitor network traffic, and timely identify and respond to abnormal activity. In addition, technologies such as network isolation [66] and segmentation can be used to reduce the attack surface and restrict the attack range;
- Implement security auditing and monitoring [67–69], detect and identify any security events through security auditing and monitoring, and respond to them promptly. Meanwhile, authenticate and control access for all users and entities accessing IoT equipment and networks to ensure that only authorized users can access the system;
- Enhance employee security awareness [70,71], strengthen employee security awareness education, and make employees aware of basic security practices such as strong passwords and anti-phishing training to reduce the occurrence of internal security threats;
- Implement emergency response plans [72,73], and develop emergency response plans to quickly identify and respond to security events. This plan should include steps to deal with vulnerabilities and malicious software, as well as how to protect critical data and information in the system.

However, these defense methods also have shortcomings. For equipment defense [62,63], it consumes a lot of resources and time, and may affect the performance and efficiency of the equipment, and cause conflicts or compatibility problems with other security software or systems, resulting in increased security risks for users. Network defense [64–66] may be identified and bypassed by malicious code, resulting in detection failure or false positives, thereby leaking user privacy data. Implementing security audit and monitoring [67–69] may block some legitimate software or programs. And employees [70,71] may be deceived and interfered with by attackers, resulting in poor or worse defense results. Implementing emergency response plans [72,73] needs to match and adapt to the security system and strategy of the enterprise, which may lead to difficulties and poor effects in information

utilization. Therefore, comprehensively adopting the above means can help IIoT systems resist APT attacks.

## 4. APT Analysis Model

In the previous section, we summarized the APTs faced by each layer of IIoT and their defense methods. In this section, we will use modeling analysis to consider factors such as the attacker's motivation, the characteristics of the target, and the attacker's technical and organizational capabilities. Here are some possible reasons for modeling and analyzing APTs.

(1) High target value: APT attacks typically target high-value targets such as government agencies, financial institutions, and military units. These targets often have a large amount of confidential information and financial resources, and once breached they can bring huge benefits.
(2) Adaptive capability: APT attackers usually use highly organized and coordinated methods to monitor and study targets for a long time and use flexible methods to launch attacks, such as social engineering or phishing emails, in order to bypass traditional security defenses.
(3) Vulnerability exploitation capability: APT attackers usually can discover and exploit vulnerabilities in the target network, such as insecure applications or incomplete network isolation, to gain more privileges and control during attacks.
(4) Persistence: APT attackers can usually exist in the target network for a long time and continue to collect and steal confidential information, making it more difficult to detect and remove APT attacks.
(5) State support: Some APT attacks are suspected to be supported by states, such as inter-state espionage activities. These attackers usually have more resources and technical support, making attacks more complex and difficult to defend against.

By establishing models and conducting analyses, we can better understand the nature and mechanisms of APT attacks and help formulate more effective defense strategies. This section will analyze APTs through six models (the threat intelligence model, attack chain model, diamond model, risk assessment model, machine learning model, and network simulation model) and make a comparison between these models.

### *4.1. Threat Intelligence Model*

Threat intelligence models are frameworks for analyzing and assessing security threats, which help organizations and security teams identify and mitigate APT attacks [74,75]. The following is an APT analysis process based on a threat intelligence model.

- Collect intelligence: Collect APT-related intelligence from various sources, such as threat intelligence platforms, open-source intelligence, hacker forums, and social media.
- Analyze intelligence: Analyze the collected intelligence to determine information about APT attack targets, methods, intentions, threats, and other aspects. This can be done using different techniques such as text analysis, statistical analysis, data mining, etc.
- Confirm the attack: Based on the analysis results, determine if there is an APT attack.
- Evaluate the threat: Evaluate the level of threat and scope of impact of the APT attack to develop appropriate response measures.
- Respond and mitigate: Based on the evaluation results, develop and implement the corresponding response and mitigation measures to reduce or eliminate the threat of the APT attack.

The authors of [75] used cyber threat intelligence (CTI) to analyze the full lifecycle of APT attacks, including collecting, analyzing, and evaluating intelligence and adopting intelligence to defend against APT attacks. The document provided an in-depth understanding and practical guidance through cases to help address APT attacks. Reference [76] used technical threat intelligence (TTI) to analyze APT attacks, providing technical analysis such as identifying attacker TTPs and revealing attack characteristics, patterns, and impacts

to provide information for defense and response. Gao et al. [77] introduced the use of open-source cyber threat intelligence (OSCTI) to analyze APT attacks, which not only helped detect and deal with APT attacks but also improved the understanding and analysis capabilities of threat intelligence to protect network security. In [78,79], structured threat information expression (STIXTM) was used to achieve network threat intelligence and information sharing, addressing the hidden dangers of using a large amount of complex network security information today. The authors [80] used STRIDE to analyze and evaluate security threats faced by systems or applications, helping developers identify and mitigate potential security risks at the design stage and improving the security of systems or applications.

To wrap up, analyzing APT attacks using a threat intelligence model is an important security task. It can help organizations understand attackers' behavior patterns, technical means, and attack goals and take targeted security measures to protect networks and sensitive data. It can also help organizations identify the types of APT attacks, evaluate the level of threat, and provide response measures. Furthermore, using a threat intelligence model to analyze APT attacks can establish a sound security system, improve security defense levels, and reduce risks and losses.

### *4.2. Attack Chain Model*

The attack chain model [81–86] is based on the attacker's analysis of the attack chain. The attack process is broken down into multiple stages, taking into account the different methods and techniques that an attacker may use. By modeling and analyzing the attack chain, potential attack paths and vulnerabilities can be identified, providing guidance for defense and response.

Different attack chain models have different divisions and naming conventions, but they typically include the following common steps.

- Reconnaissance: The attacker gathers information about the target, such as IP addresses, operating systems, and vulnerabilities.
- Weaponization: The attacker creates malicious payloads, such as Trojans, backdoors, and ransomware, and combines them with transmission carriers such as emails, web pages, and documents.
- Delivery: The attacker sends the malicious payload to the target or lures the target to visit a malicious website.
- Exploitation: The malicious payload exploits vulnerabilities in the target system or user actions to execute malicious code.
- Installation: Malicious code installs backdoors or other malware on the target system for persistent control.
- Command and control: The malware communicates with the attacker's remote server, receiving instructions, or sending data.
- Execution: The malware executes the final goal according to the attacker's instructions, such as stealing data, destroying the system, or spreading ransomware.

Different attack chain models may divide or merge these steps or add additional steps to adapt to different scenarios and requirements. Table 4 shows some common attack chain models and their developments.

The attack chain model is a useful way to analyze APT attacks, which can help us better understand the attackers' behavior and intent and detect and respond to attack activities in a timely manner. By using the attack chain model, we can gain insight into the attackers' attack strategy, improve overall security, identify threats, discover vulnerabilities, and take preventive measures in time.

**Table 4.** Attack chain model and its development.

| Model | Step | Characteristic |
| --- | --- | --- |
| Lockheed Martin network kill chain [81,82] | Reconnaissance, weaponization, delivery, utilization, installation, command and control, and action | Based on military terminology, it is assumed that the attacker performs the steps in a linear order with malware as the center |
| MITRE ATT and CK [83,84] | Initial access, execution, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, aggregation, penetration testing, and impact | Pay attention to the attacker's tactics, techniques, and procedures, which are nonlinear, finer-grained, and more comprehensive |
| Unified kill chain [85] | Reconnaissance, weaponization, delivery, utilization, installation, command, and control, action target selection, data collection, data leakage, and data destruction | Combining the advantages of Lockheed Martin and MITRE, the target and behavior of the attacker are described in more detail |
| XDR framework/ attack chain [86] | Reconnaissance, weaponization/delivery/utilization, command and control/action, and abnormal user behavior | Adapt to the framework of the XDR platform, pay attention to threat detection and response across terminals, networks, and clouds, and ignore traditional steps |

### *4.3. Diamond Model*

The diamond model [87] is a framework used for analyzing advanced persistent threats (APTs). It consists of four key elements: the adversary, infrastructure, victim, and action. According to the diamond model, in APT attacks, the adversary targets specific victims using its controlled infrastructure and capabilities to achieve its objectives. The attacker and infrastructure are the initiating factors, while the victim and action are the targets and results of the attack. The following is a detailed explanation of the diamond model for APTs [88,89].

- Adversary: Refers to the person or organization that initiates the APT attack. They typically have clear intentions, as well as the technical and resource capabilities to execute long-term, covert, and complex attacks. Understanding the characteristics and capabilities of the adversary is essential for predicting their next actions and taking appropriate defense measures.
- Infrastructure: Refers to the hardware and software resources used by the attacker. This includes CC servers, botnets, malware, exploitation tools, and encryption technologies. The attacker's infrastructure often changes and evolves to avoid detection and monitoring by security defense measures.
- Victim: Refers to the person or organization that suffers the APT attack. Victims can be government agencies, military organizations, businesses, or individuals. APT attacks typically use social engineering, exploit vulnerabilities, use phishing attacks, and use other methods to obtain sensitive information or disrupt the victim's systems, thereby achieving their attack objectives.
- Action: Refers to the specific actions taken by the attacker during the incident, such as stealing confidential information, damaging systems, or monitoring the victim. Understanding the attacker's actions can help the victim assess the extent of the

damage and take measures to repair their system and prevent similar attacks from occurring again.

The work [90] used the diamond model to analyze APTs; discussed the social and political background and intention of APTs; and helped us understand the core issues of APT activities, such as who, what, when, where, why, and how. References [91,92] used the diamond model to analyze the characteristics and behavior of APTs and how to use the diamond model combined with attribution technology to detect and defend against APTs.

To sum up, the diamond model provides a comprehensive and systematic method to analyze and understand APTs. By analyzing the relationship between attackers, the infrastructure, victims, and actions, victims can be helped to better manage risks, thus protecting their sensitive information and property from the threat of attacks.

### *4.4. Risk Assessment Model*

Risk assessment models are used to quantify threats in IIoT systems, in order to determine which threats pose a greater risk to system security and prioritize their mitigation. For example, the risk matrix model [93] is a method of classifying and evaluating risks based on probability and impact, helping decision-makers identify and manage risks. The risk index model [94] calculates a risk index by combining factors such as the likelihood of a risk occurring, its impact, and sensitivity, to reflect the size and severity of the risk. The risk-scoring model [95] is a method used to predict the probability of an event or disease occurring, by calculating a risk score based on relevant risk factors. The STRIDE model [96] categorizes threats into six categories, including spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege, helping analysts to understand and identify system security threats from the attacker's perspective and formulate corresponding mitigation measures.

Regarding the node-level epidemic model [97,98], nodes represent people or things, and infectious diseases represent malware or attacks . In IIoT, nodes can be equipment or sensors connected to the system, while malware can be malicious code or attackers. By simulating the spread of APTs in IIoT, organizations can understand how APT attacks spread and determine how to reduce the impact of attacks. Park et al. [99] put forward an evaluation method, which describes the situation of APT attacks with a problem domain ontology and could evaluate the risk of an APT attack on an organization. The work [100] used an algorithm to predict the security risk of each node in the network, effectively evaluated the security situation of the network, helped the defender to take measures to prevent APT attacks, and improved the security of the network.

In conclusion, risk assessment models can help identify and evaluate the likelihood, impact, and losses of APT attacks and formulate corresponding defense strategies and response measures. Risk assessment models can enhance network security awareness and capabilities and strengthen prevention and resistance to APT attacks. Risk assessment models can provide a scientific basis and guidance for network security management and optimize resource allocation and input–output ratios.

### *4.5. Machine Learning Model*

Machine learning models [101,102] are functions that can learn features and patterns from data, which can be used to analyze APT attack behavior for classification, prediction, clustering, association, and other purposes. For example, supervised learning algorithms such as support vector machines (SVM) [103], decision trees [104], and random forests [102], and unsupervised learning algorithms such as clustering [105] and anomaly detection [106], can be used to classify and predict, or detect, abnormal behavior and potential threats in the system.

The advantages of using machine learning models to analyze APTs are the automation of processing a large number of data and improving analysis efficiency and accuracy.

The ability to use multiple data sources such as network traffic, logs, malware, and intelligence improves analysis comprehensiveness and depth. Adaptation to constantly

changing threat environments improves analysis sensitivity and robustness through the continuous updating and optimization of models. To sum up, using machine learning models to analyze APT attacks has multiple advantages, which can improve system security and stability and help organizations effectively respond to APT attacks.

### *4.6. Network Simulation Model*

Network simulation is a method of simulating network operations that can help us test, evaluate, optimize network performance, predict network behavior, and validate new network solutions [107]. Commonly used network simulation tools include NS-3 (Network Simulator 3), OPNET (optimized network engineering tool), OMNeT++, MATLAB, Simulink, GNS3, Riverbed Modeler, NetSim, QualNet, and Cisco Packet Tracer [108,109].

NS-3 is an open-source and highly modular network simulator that provides modules for many network protocols and supports advanced network models and topologies. OPNET is a commercial network simulation tool that provides multiple simulation capabilities, including network design, performance analysis and optimization, network security, and more. OMNeT++ is an open-source network simulator that supports various network technologies, including wireless networks, mobile networks, and the Internet. MATLAB Simulink is a commercial simulation tool that can be used for network system design, control system design, signal processing, and more. GNS3 is a free and open-source network simulation tool that can simulate various types of network equipment such as routers and switches and supports the simulation of multiple network protocols. Riverbed Modeler is a commercial network simulation tool that can be used for network design, performance optimization, traffic analysis, and more. NetSim is a commercial network simulation tool that can be used for network design, performance evaluation, fault diagnosis, and more. QualNet is a commercial network simulation tool that can be used for simulating wireless networks, satellite networks, mobile networks, sensor networks, and more. Cisco Packet Tracer is a free network simulation tool that can be used for simulating network topology and configuring network equipment.

Network simulation models can provide a secure, controllable, and repeatable experimental environment for simulating various stages and techniques of APT attacks, as well as defensive measures and response strategies for the target network [110,111]. Network simulation models can help network security personnel and researchers gain a deeper understanding of the principles, characteristics, behavior, and impact of APT attacks, as well as assess the level of threat and risk evaluation posed by APT attacks to the target network [112,113]. Network simulation models can help network security personnel and researchers design and validate new APT detection, prevention, response, and traceability methods, as well as evaluate their effectiveness and performance [114,115]. Network simulation models can also help network security personnel and researchers conduct education and training on APT attacks to improve network security awareness and capability [116,117].

To summarize, network simulation models are based on simulating industrial IoT systems and simulating the impact and propagation of different advanced persistent threats on the system to evaluate the security performance and vulnerability of the system. By simulating and analyzing different attack scenarios, enterprises can understand the threat propagation mechanisms, scope of impact, and damage caused by APTs and optimize the security defense of the system.

### *4.7. Model Comparison*

Through the detailed description of the six models above, we summarize that the advantage of the threat intelligence model [74,75] is that it can provide targeted and practical threat intelligence information and help organizations formulate effective security strategies and measures, and its disadvantage is that it relies on external sources of information, which may lead to the low quality, timeliness, and reliability of the information. The application of the threat intelligence model to defend against APT attacks lies in the fact that it can help

organizations obtain and use the threat intelligence information of APT attacks in time, thereby improving the early warning and response capabilities for APT attacks. The advantage of the attack chain model [81–86] is that it can provide a clear and complete view of the attack process and help organizations take corresponding defense measures at different stages, and its disadvantage is that it may not cover all types and changes of attack methods and may also be identified and avoided by attackers. The application of the attack chain model to defend against APT attacks lies in the fact that it can help security personnel analyze the behavior and purpose of attackers. The advantage of the diamond model [87–89] is that it can provide a comprehensive and dynamic view of competitive analysis and help organizations discover their own and others' strengths and weaknesses, and its disadvantage is that it may ignore some important factors, such as government policies, cultural differences, and international cooperation. The application of the diamond model to defend against APT attacks lies in the fact that it can help organizations understand the various factors that affect APT activities. The advantage of the risk assessment model [93–96] is that it can provide a systematic and scientific view of risk management and help organizations formulate reasonable and effective risk control measures, and its disadvantage is that it may be affected by data quality, assessment methods, human factors, etc., resulting in inaccurate or incomplete assessment results. The ability of the risk assessment model to defend against APT attacks lies in the fact that it can help organizations assess and control the risks associated with APT attacks. The advantage of the machine learning model [101–106] is that it can provide an efficient and flexible view of data analysis, help organizations discover hidden information and value in data, and its disadvantage is that it may be affected by data quality, algorithm selection, model training, etc., resulting in poor or unstable model performance. The application of the machine learning model to defend against APT attacks lies in the fact that it can help organizations process and use large and diverse data, such as network traffic, log files, and threat intelligence, thereby improving the detection and analysis capabilities for APT attacks. The advantage of the network simulation model [107–109] is that it can provide a controllable and repeatable network experiment environment and help organizations analyze and understand the interaction between different network components and devices, and its disadvantage is that it may not fully reflect all factors and situations in real networks and may also have some errors and biases. The application of the network simulation model to defend against APT attacks lies in the fact that it can help organizations design and verify new network protocols, algorithms, architectures, etc., thereby improving their defense capabilities against APT attacks.

In order to better and more intuitively understand these six models, we list their advantages, disadvantages, and applications in Table 5.

**Table 5.** Advantages, disadvantages, and applications of models.

| Model | Advantages | Disadvantages | Applications |
|---|---|---|---|
| Threat intelligence model | Provide targeted and practical information | The quality, timeliness, and reliability of information are not high | Early warning and response-ability with regard to APTs |
| Attack chain model | Clear and complete view of attack process | May be recognized and evaded by attackers | Analyze the behavior and purpose of attackers |
| Diamond model | Comprehensive and dynamic APT analysis view | Will ignore some important factors | Understand the various factors that affect APTs |
| Risk assessment model | Help organizations formulate reasonable and effective measures | Affected by data quality, evaluation methods, and human factors | Assess and control the risks associated with APTs |

**Table 5.** *Cont.*

| Model | Advantages | Disadvantages | Applications |
| --- | --- | --- | --- |
| Machine learning model | Discover hidden information and value in data | Affected by data quality, algorithm selection, and model training | Process and utilize a large number and variety of data |
| Network simulation model | Analyze and understand the interaction between networks and equipment | Cannot fully reflect the real network | Design and verify new network |

## 5. Work Comparison

In this section, we will review the most important previous works of this type about the position of APTs in a brief and concise form about what they achieved and what new ideas they presented.

### *5.1. Technique Study*

Network security researchers put forward some important research ideas in the battle with APTs, which they think are the most advanced and complete strategies [118]. However, a closer study shows that the proposed architecture is incomprehensible and cannot adapt to the complex and ever-changing network threat scenarios. Table 6 shows the complete inspection of various APT detection and prevention strategies proposed by well-known researchers. In order to fully understand the threat situation of APTs, we summarized the advantages and disadvantages of each technology.

**Table 6.** Famous techniques preventing APTs.

| Article (Year) | Techniques | Advantages | Limitations |
| --- | --- | --- | --- |
| [77] (2021) | OSCTI | (1) Natural language processing pipeline is unsupervised, light-weight, and accurate; (2) can automatically synthesize a based-on system audit query; and (3) has an efficient query execution engine | (1) Reliability of information sources; (2) information overload, redundancy; and (3) privacy and risk of information |
| [84] (2020) | MITRE ATT and CK | (1) Directly applied to attack diagnosis and threat mitigation; (2) is highly predictable against APT attacks | (1) Quantity and quality assurance of real attack data sets; (2) a lot of time, manpower, capital, and other resources lead to the high cost or low efficiency |
| [91] (2022) | Diamond model | (1) Help organization identify and track attacker behaviour and targets; (2) help organizations share and exchange threat intelligence information; and (3) reflect the current threat environment and trends | (1) Inability to cover changing cyber attacks; (2) information is difficult to filter, collate, and analyze |
| [99] (2021) | Risk assessment model | (1) Risk assessment against predictable attacks; (2) assesses the relative risk of multiple APT attacks; and (3) helps to establish a proactive security strategy | (1) The need to fully understand the characteristics of intelligent and sophisticated attacks; (2) different assessments for specific APT attacks |
| [102] (2021) | Random forest | (1) Achieved good results in detecting APTs; (2) performed better feature selection and extraction | (1) Large number of high-quality data required; (2) limited scope for APT attack detection |
| [114] (2022) | Network simulation | (1) Provide a controlled and repeatable network experimental environment; (2) analyze complex network environments | (1) Some deviation from real APTs; (2) high-cost of model construction and maintenance |

### *5.2. Survey Discussion*

In [119], the authors surveyed the different types of attacks that an attacker can launch against IIoT equipment and mentioned ways to mitigate such attacks. In work [120], the

authors reviewed intrusion-detection and -prevention mechanisms in the IIoT domain and highlight different protocols, algorithms, and mechanisms. In addition, they compared different mechanisms used to detect, prevent, and secure IIoT systems. In work [121], the authors summarized a lifecycle-based approach to APT attacks to address APTs. They further proposed an APT detection method using machine learning techniques, and the proposed model was divided into two passive phases and three active phases. Mei et al. [122] provided an overview of APT attacks in terms of their origin and definition; introduced the attack mechanism, the attack process, and the attack techniques used in each phase; and classified the detection and defense techniques available in different attack phases to provide a reference for further defense research. Sengupta et al. [123] classified the attacks according to the vulnerability object. The individual attacks were then mapped to one or more layers of the IIoT architecture to enable further discussion of proposed countermeasures against the most relevant security threats in the industrial internet of things . Our work examines the types of APT attacks as well as the APT attacks and defense techniques that each layer of the IIoT reference architecture may face. Further, we use several models to simulate and analyze APT activities in the IIoT.

However, few people have comprehensively studied and solved the problem of defending against APT attacks. In order to ensure the novelty and new contribution of our investigation, we have thoroughly compared our work with the existing survey, as shown in Table 7.

**Table 7.** Advantages, disadvantages, and applications of models.

| Survey | Article (Year) | Objective | Prospect |
|---|---|---|---|
| A survey on the classification of cyber-attacks on IoT and IIoT devices | [119] (2020) | Aims to recognize the different Cyber-attacks, which are related to IIoT equipment and fully securing IIoT | Must understand the different Cyber-attacks that an IIoT network faces to develop new protection mechanisms |
| Intrusion detection and prevention in industrial IoT: a technological survey | [120] (2021) | Detect, prevent, and protect IIoT systems from different vulnerabilities, threats, and attacks | Expanding the use of artificial intelligence, 5G and blockchain technologies for IIoT security |
| A new proposal on the advanced persistent threat: A survey | [121] (2020) | Proposing a new APT detection model using machine learning techniques | A framework based on the proposed five-stage model is proposed. Also, build data sets to train the ML algorithms used in the framework |
| A survey of advanced persistent threats: attack and defense | [122] (2021) | Introduction to the various stages of attack techniques and classification of detection and defense techniques | Research for more APT attack models |
| A comprehensive survey on attacks, security issues, and blockchain solutions for IoT and IIoT | [123] (2020) | Design the classification of IIoT security research fields and the corresponding solutions | Develop robust security solutions to address emerging threats with the latest technology |
| Our work | - | Overview and modeling analysis of APT attacks and defenses for each layer of the IIoT system | Combining APT detection technology, blockchain, 5G, AI, and big data to defend against ever-evolving APTs |

## 6. Open Research Problem

IIoT security issues cover a range of IIoT systems, from the physical security of connected nodes or equipment; network communication security; and data security during transmission, transformation, and storage processes, to application security. Due to the highly specialized nature of APTs, it is questionable whether traditional mechanisms are still sufficient to protect recent IIoTs, and this section will discuss open research issues in APTs faced by IIoTs.

- The focus of the work is to ensure specific IIoT architecture, including a network-physical-social-based security model [124], focusing on the U2IoT architecture [125]

and secure method grid designed to protect SDN-based IIoT architectures [126]. As a single security architecture and framework cannot fix the entire IIoT system, a bottom-up approach is needed to design IIoT security architectures with higher levels of abstraction. The emphasis of the proposal should be on interoperability issues to integrate different security mechanisms supported by IIoT technology and cross-layer security solutions.

- The limitations of traditional point-to-point defense systems and security mechanisms. The connections and communications between IIoT networks have recently been protected using traditional network security protocols such as TLS/SSL, IPSec, RADIUS, and IKE. Most of these security protocols are based on point-to-point defense. For example, TLS/SSL provides transport layer protection, and IPSec focuses on the MAC, data link, transport, and network layer of IPv6 and IPv4. As IIoT communication technologies become more diverse, these traditional security mechanisms, which focus on point-to-point defense, are less effective against APT attacks. APT attacks can target any vulnerabilities or weak links in IIoT and application systems, and equipment that has been hijacked or installed with backdoors can easily infiltrate the IIoT.
- Lightweight and stronger encryption algorithms. Most IIoT communication protocols and technologies still rely on traditional encryption algorithms such as RSA, MD5, RC4, and DES-56 to ensure data confidentiality and communication security. However, some of these algorithms have been proven to be insecure against quantum attacks. Therefore, a more robust encryption algorithm is needed to adapt to these communication protocols, such as quantum-resistant NTRU and BLISS algorithms. In addition, a lightweight but secure algorithm is highly sought after to protect the limited resources of industrial IoT (e.g., low-energy, low-storage, and low-bandwidth communication). For example, RC5, SkipJack, high security lightweight (HIGHT), modified block TEA (XXTEA), and SAFER++ have recently been proposed to protect wireless sensor networks [127,128].
- Data-centric approach. The data-centric approach aims to protect the data itself, rather than targeting different networks, communication technologies, and protocols for protection, regardless of when and where. As there is no single security mechanism and framework that can cover the entire industrial IoT ecosystem, data-centric approaches can serve as an alternative solution for IIoT end-to-end security. These data-centric approaches include homomorphic encryption, attribute-based encryption schemes, private information retrieval schemes, searchable encryption schemes, and multiparty computation schemes [129,130]. These schemes mostly ensure the security of data in transit, data in transformation, and static data, thus greatly addressing interoperability and scalability issues across IIoT and technology integration with different security mechanisms.
- Investigate the hacker community. In addition, investigating the hacker community can help identify zero-day vulnerabilities before they are exploited. According to [131,132], some vulnerabilities have been discussed by the black hat community before being publicly exposed by ethical organizations. Hackers interact and communicate with each other through forums, which are user-oriented platforms whose sole purpose is to enable communication among hackers around the world. These so-called dark web forums are usually very similar to other normal web forums, where they discuss programming, hacking, and network security [133,134]. These forums provide an opportunity for hackers from around the world to exchange their findings, customized tools, and malware. The existence of such hacker communities is common in various geopolitical regions, including the United States, Russia, the Middle East, China, and other regions. This is an increasingly serious global problem. Research in this area has the potential to have a huge social impact [135].
- Cloud computing. Another area that affects APT defense systems is cloud computing. Cloud computing provides different types of services and resources that can be used to send, store, or process data. For defense systems for organizations without cloud

resources, they can monitor data leakage to unknown or external IPs. However, for organizations with cloud resources, detecting leakage activities can be very challenging, and this is an area that needs to be explored due to the multiple cloud resources and services that can be used to leak data. The proposed defense system should have a strong correlation model that can correlate interrelated activities involving stealing organizational data. For example, attackers can use the target organization's cloud storage service to steal data instead of sending data directly to their command and control center through the organization's network. Using storage services requires attackers to steal the credentials of cloud users in the organization who have permission to place or retrieve objects from that storage service. Once credentials are stolen, they can upload data to storage resources and download data to their command and control center without being detected using the same credentials.

## 7. Conclusions

This paper first describes the definition and development of APTs. On the basis of this, we analyze the APT threats and research status faced by each layer of architecture in IIoT and review the defense techniques against APTs. Then, we use a variety of models to analyze the essence of APT activities, to improve the security protection capabilities of IIoT. Finally, based on the in-depth discussion of IIoT security issues, we propose some open research topics. The limitations of this survey are the lack of detection and identification of APT attacks and the exploitation of emerging information technologies. With this, we should next combine APT detection and identification technologies, blockchain, 5G, AI, and big data to defend against evolving APTs.

**Author Contributions:** Conceptualization, methodology, writing—original draft preparation, writing—review and editing, C.G. and J.L.; Conceptualization, resources, supervision, D.-W.H.; Methodology, software, validation, supervision, Q.Z. and L.T. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was supported by the Research Innovation Program for Postgraduate of Chongqing (No. CYS23445), and the Chongqing Research Program of Basic Research and Frontier Technology (No. cstc2021jcyj-msxmX0761).

**Data Availability Statement:** No new data were created or analyzed in this study. Data sharing is not applicable to this article.

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

## References

1. Serror, M.; Hack, S.; Henze, M.; Schuba, M.; Wehrle, K. Challenges and opportunities in securing the industrial internet of things. *IEEE Trans. Ind. Inform.* **2020**, *17*, 2985–2996. [CrossRef]
2. Lu, Y.; Li, J.; Zhang, Y. Privacy-preserving and pairing-free multirecipient certificateless encryption with keyword search for cloud-assisted IIoT. *IEEE Internet Things J.* **2019**, *7*, 2553–2562. [CrossRef]
3. Malik, P.K.; Sharma, R.; Singh, R.; Gehlot, A.; Satapathy, S.C.; Alnumay, W.S.; Pelusi, D.; Ghosh, U.; Nayak, J. industrial internet of things and its applications in industry 4.0: State of the art. *Comput. Commun.* **2021**, *166*, 125–139. [CrossRef]
4. Hussain, Z.; Akhunzada, A.; Iqbal, J.; Bibi, I.; Gani, A. Secure IIoT-Enabled Industry 4.0. *Sustainability* **2021**, *13*, 12384. [CrossRef]
5. Yu, K.; Tan, L.; Mumtaz, S.; Al-Rubaye, S.; Al-Dulaimi, A.; Bashir, A.; Khan, F.A. Securing Critical Infrastructures: Deep-Learning-Based Threat Detection in IIoT. *IEEE Commun. Mag.* **2021**, *59*, 76–82. [CrossRef]
6. Baldelovar, M.A.; Komarasamy, G. A Study into the Security Issues and Countermeasures for the industrial internet of things (IIOT). *Technoarete Trans. Internet Things Cloud Comput. Res.* **2022**, *2*, 8–13. [CrossRef]
7. Stojanović, B.; Hofer-Schmitz, K.; Kleb, U. APT datasets and attack modeling for automated detection methods: A review. *Comput. Secur.* **2020**, *92*, 101734. [CrossRef]
8. Xing, K.; Li, A.; Jiang, R.; Jia, Y. A Review of APT Attack Detection Methods and Defense Strategies. In Proceedings of the 2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC), Hong Kong, China, 27–30 July 2020; pp. 67–70.
9. Liao, X.; Faisal, M.; QingChang, Q.; Ali, A.; Khan, H.U. Evaluating the Role of Big Data in IIOT-industrial internet of things for Executing Ranks Using the Analytic Network Process Approach. *Sci. Program.* **2020**, *2020*, 1–7. [CrossRef]
10. Alferidah, D.K.; Jhanjhi, N. A review on security and privacy issues and challenges in internet of things. *Int. J. Comput. Sci. Netw. Secur. IJCSNS* **2020**, *20*, 263–286.

11. Hoffmann, M.; Kryszkiewicz, P. Signaling Storm Detection in IIoT Network based on the Open RAN Architecture. *arXiv* **2023**, arXiv:2302.08239.
12. O'Raw, J.; Laverty, D.; Morrow, D.J. Securing the industrial internet of things for critical infrastructure (IIoT-CI). In Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 15–18 April 2019; pp. 70–75.
13. Mouratidis, H.; Diamantopoulou, V. A security analysis method for industrial internet of things. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4093–4100. [CrossRef]
14. Qi, L.; Yang, Y.; Zhou, X.; Rafique, W.; Ma, J. Fast anomaly identification based on multiaspect data streams for intelligent intrusion detection toward secure industry 4.0. *IEEE Trans. Ind. Inform.* **2021**, *18*, 6503–6511. [CrossRef]
15. Yang, H.; Cheng, L.; Chuah, M.C. Deep-learning-based network intrusion detection for SCADA systems. In Proceedings of the 2019 IEEE Conference on Communications and Network Security (CNS), Washington, DC, USA, 10–12 June 2019; pp. 1–7.
16. Coppolino, L.; D'Antonio, S.; Mazzeo, G.; Romano, L. A comprehensive survey of hardware-assisted security: From the edge to the cloud. *Internet Things* **2019**, *6*, 100055. [CrossRef]
17. Kalunga, J.; Tembo, S.; Phiri, J. industrial internet of things common concepts, prospects and software requirements. *Int. J. Internet Thing* **2020**, *9*, 1.
18. Younan, M.; Houssein, E.H.; Elhoseny, M.; Ali, A.A. Challenges and recommended technologies for the industrial internet of things: A comprehensive review. *Measurement* **2020**, *151*, 107198. [CrossRef]
19. Mrabet, H.; Alhomoud, A.; Jemai, A.; Trentesaux, D. A Secured Industrial Internet-of-Things Architecture Based on Blockchain Technology and Machine Learning for Sensor Access Control Systems in Smart Manufacturing. *Appl. Sci.* **2022**, *12*, 4641. [CrossRef]
20. Ahlmeyer, M.; Chircu, A.M. Securing the Internet of Things: A review. *Issues Inf. Syst.* **2016**, *17*, 21–28.
21. Hassanzadeh, A.; Modi, S.; Mulchandani, S. Towards effective security control assignment in the Industrial Internet of Things. In Proceedings of the 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy, 14–16 December 2015; pp. 795–800.
22. Vijayakumaran, C.; Muthusenthil, B.; Manickavasagam, B. A reliable next generation cyber security architecture for industrial internet of things environment. *Int. J. Electr. Comput. Eng.* **2020**, *10*, 387. [CrossRef]
23. Javed, S.H.; Ahmad, M.B.; Asif, M.; Almotiri, S.H.; Masood, K.; Ghamdi, M.A.A. An intelligent system to detect advanced persistent threats in industrial internet of things (I-IoT). *Electronics* **2022**, *11*, 742. [CrossRef]
24. Shi, Y.; Li, W.; Zhang, Y.; Deng, X.; Yin, D.; Deng, S. Survey on APT Attack Detection in Industrial Cyber-Physical System. In Proceedings of the 2021 International Conference on Electronic Information Technology and Smart Agriculture (ICEITSA), Huaihua, China, 10–12 December 2021; pp. 296–301.
25. Bagaa, M.; Taleb, T.; Bernabe, J.B.; Skarmeta, A. A machine learning security framework for iot systems. *IEEE Access* **2020**, *8*, 114066–114077. [CrossRef]
26. Latif, S.; Driss, M.; Boulila, W.; Huma, Z.; Jamal, S.S.; Idrees, Z.; Ahmad, J. Deep Learning for the industrial internet of things (IIoT): A Comprehensive Survey of Techniques, Implementation Frameworks, Potential Applications, and Future Directions. *Sensors* **2021**, *21*, 7518. [CrossRef] [PubMed]
27. Miloslavskaya, N.; Tolstoy, A. Internet of Things: Information security challenges and solutions. *Clust. Comput.* **2019**, *22*, 103–119. [CrossRef]
28. Wang, H.; Chen, Z.; Zhao, J.; Di, X.; Liu, D. A vulnerability assessment method in industrial internet of things based on attack graph and maximum flow. *IEEE Access* **2018**, *6*, 8599–8609. [CrossRef]
29. George, G.; Thampi, S.M. A graph-based security framework for securing industrial IoT networks from vulnerability exploitations. *IEEE Access* **2018**, *6*, 43586–43601. [CrossRef]
30. Abomhara, M.; Køien, G.M. Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. *J. Cyber Secur. Mobil.* **2015**, 65–88. [CrossRef]
31. Panchal, A.C.; Khadse, V.M.; Mahalle, P.N. Security issues in IIoT: A Comprehensive Survey Of Attacks on IIoT and its Countermeasures. In Proceedings of the 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), Lonavala, India, 23–24 November 2018; pp. 124–130.
32. Kumar, A.; Thing, V.L. RAPTOR: Advanced Persistent Threat Detection in Industrial IoT via Attack Stage Correlation. *arXiv* **2023**, arXiv:2301.11524.
33. Karnouskos, S. Stuxnet Worm Impact On Industrial Cyber-Physical System Security. In Proceedings of the IECON 2011–2037th Annual Conference of the IEEE Industrial Electronics Society, Melbourne, VIC, Australia, 7–10 November 2011; pp. 4490–4494.
34. Falliere, N.; Murchu, L.O.; Chien, E. W32. stuxnet dossier. *White Pap. Symantec Corp. Secur. Response* **2011**, *5*, 29.
35. McFail, M.; Hanna, J.; Rebori-Carretero, D. *Detection Engineering in Industrial Control Systems. Ukraine 2016 Attack: Sandworm Team and Industroyer Case Study*; Technical Report; MITRE Corporation: McLean, VA, USA, 2021; pp. 2–3.
36. Di Pinto, A.; Dragoni, Y.; Carcano, A. TRITON: The first ICS cyber attack on safety instrument systems. *Proc. Black Hat USA* **2018**, *2018*, 1–26.
37. Sapalo Sicato, J.C.; Sharma, P.K.; Loia, V.; Park, J.H. VPNFilter malware analysis on cyber threat in smart home network. *Appl. Sci.* **2019**, *9*, 2763. [CrossRef]
38. Adamov, A.; Carlsson, A.; Surmacz, T. An analysis of lockergoga ransomware. In Proceedings of the 2019 IEEE East-West Design & Test Symposium (EWDTS), Batumi, Georgia, 13–16 September 2019; pp. 1–5.
39. Abd Elazeem, N.E. Effect of cybercrime on the pharmaceutical industry. *J. Intellect. Prop. Innov. Manag.* **2020**, *3*, 91–121. [CrossRef]

40. Sparkes, M. How do we solve the problem of ransomware? *New Sci.* **2021**, *250*, 13. [CrossRef]
41. Szymanski, T.H. Supporting consumer services in a deterministic industrial internet core network. *IEEE Commun. Mag.* **2016**, *54*, 110–117. [CrossRef]
42. Atzori, L.; Iera, A.; Morabito, G. The internet of things: A survey. *Comput. Netw.* **2010**, *54*, 2787–2805. [CrossRef]
43. Liu, C.H.; Yang, B.; Liu, T. Efficient naming, addressing and profile services in Internet-of-Things sensory environments. *Ad Hoc Netw.* **2014**, *18*, 85–101. [CrossRef]
44. Tan, S.; Samsudin, A. Recent Technologies, Security Countermeasure and Ongoing Challenges of industrial internet of things (IIoT): A Survey. *Sensors* **2021**, *21*, 6647. [CrossRef]
45. Latif, S.; Idrees, Z.; e Huma, Z.; Ahmad, J. Blockchain technology for the industrial internet of things: A comprehensive survey on security challenges, architectures, applications, and future research directions. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4337. [CrossRef]
46. Latif, S.; Zou, Z.; Idrees, Z.; Ahmad, J. A novel attack detection scheme for the industrial internet of things using a lightweight random neural network. *IEEE Access* **2020**, *8*, 89337–89350. [CrossRef]
47. Mahmoud, R.; Yousuf, T.; Aloul, F.; Zualkernan, I. 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), London, UK, 14–16 December 2015; pp. 336–341.
48. Khan, S.; Altayar, M. industrial internet of things: Investigation of the applications, issues, and challenges. *Int. J. Adv. Appl. Sci.* **2021**, *8*, 104–113. [CrossRef]
49. Li, S.; Tryfonas, T.; Li, H. The Internet of Things: A security point of view. *Internet Res.* **2016**, *26*, 337–359. [CrossRef]
50. Sadeghi, A.R.; Wachsmann, C.; Waidner, M. Security and privacy challenges in industrial internet of things. In Proceedings of the 52nd Annual Design Automation Conference, San Francisco, CA, USA, 7–11 June 2015; pp. 1–6.
51. Ngo, Q.D.; Nguyen, H.T.; Le, V.H.; Nguyen, D.H. A survey of IoT malware and detection methods based on static features. *ICT Express* **2020**, *6*, 280–286. [CrossRef]
52. Naeem, H.; Ullah, F.; Naeem, M.R.; Khalid, S.; Vasan, D.; Jabbar, S.; Saeed, S. Malware detection in industrial internet of things based on hybrid image visualization and deep learning model. *Ad Hoc Netw.* **2020**, *105*, 102154. [CrossRef]
53. Da Costa, K.A.; Papa, J.P.; Lisboa, C.O.; Munoz, R.; de Albuquerque, V.H.C. Internet of Things: A survey on machine learning-based intrusion detection approaches. *Comput. Netw.* **2019**, *151*, 147–157. [CrossRef]
54. Sisinni, E.; Saifullah, A.; Han, S.; Jennehag, U.; Gidlund, M. industrial internet of things: Challenges, opportunities, and directions. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4724–4734. [CrossRef]
55. Silva, B.N.; Khan, M.; Han, K. Internet of things: A comprehensive review of enabling technologies, architecture, and challenges. *IETE Tech. Rev.* **2018**, *35*, 205–220. [CrossRef]
56. Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of Things security: A survey. *J. Netw. Comput. Appl.* **2017**, *88*, 10–28. [CrossRef]
57. Huma, Z.E.; Latif, S.; Ahmad, J.; Idrees, Z.; Ibrar, A.; Zou, Z.; Alqahtani, F.; Baothman, F. A hybrid deep random neural network for cyberattack detection in the industrial internet of things. *IEEE Access* **2021**, *9*, 55595–55605. [CrossRef]
58. Berger, S.; Bürger, O.; Röglinger, M. Attacks on the industrial internet of things–Development of a multi-layer Taxonomy. *Comput. Secur.* **2020**, *93*, 101790. [CrossRef]
59. Ding, W.; Jing, X.; Yan, Z.; Yang, L.T. A survey on data fusion in internet of things: Towards secure and privacy-preserving fusion. *Inf. Fusion* **2019**, *51*, 129–144. [CrossRef]
60. Abdo, H.; Kaouk, M.; Flaus, J.M.; Masse, F. A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie–combining new version of attack tree with bowtie analysis. *Comput. Secur.* **2018**, *72*, 175–195. [CrossRef]
61. Malani, S.; Srinivas, J.; Das, A.K.; Srinathan, K.; Jo, M. Certificate-based anonymous device access control scheme for IoT environment. *IEEE Internet Things J.* **2019**, *6*, 9762–9773. [CrossRef]
62. Lesjak, C.; Hein, D.; Winter, J. Hardware-Security Technologies For Industrial IoT: TrustZone and Security Controller. In Proceedings of the IECON 2015–2041st Annual Conference of the IEEE Industrial Electronics Society, Yokohama, Japan, 9–12 November 2015; pp. 2589–2595.
63. Pinto, S.; Gomes, T.; Pereira, J.; Cabral, J.; Tavares, A. IIoTEED: An enhanced, trusted execution environment for industrial IoT edge devices. *IEEE Internet Comput.* **2017**, *21*, 40–47. [CrossRef]
64. Pretorius, B.; van Niekerk, B. IIoT Security: Do I Really Need a Firewall for my Train? In Proceedings of the ICCWS 2019 14th International Conference on Cyber Warfare and Security: ICCWS 2019, Stellenbosch, South Africa, 28 February–1 March 2019; pp. 338–347.
65. Alsaedi, A.; Moustafa, N.; Tari, Z.; Mahmood, A.; Anwar, A. TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems. *IEEE Access* **2020**, *8*, 165130–165150. [CrossRef]
66. Basta, N.; Ikram, M.; Kaafar, M.A.; Walker, A. Towards a Zero-Trust Micro-Segmentation Network Security Strategy: An Evaluation Framework. In Proceedings of the NOMS 2022–2022 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, 25–29 April 2022; pp. 1–7.
67. Goldenberg, N.; Wool, A. Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems. *Int. J. Crit. Infrastruct. Prot.* **2013**, *6*, 63–75. [CrossRef]

68. Hadžiosmanović, D.; Sommer, R.; Zambon, E.; Hartel, P.H. Through the Eye of the PLC: Semantic Security Monitoring for Industrial Processes. In Proceedings of the 30th Annual Computer Security Applications Conference, Louisiana, NO, USA, 8–12 December 2014; pp. 126–135.
69. Zhou, C.; Huang, S.; Xiong, N.; Yang, S.H.; Li, H.; Qin, Y.; Li, X. Design and analysis of multimodel-based anomaly intrusion detection systems in industrial process automation. *IEEE Trans. Syst. Man Cybern. Syst.* **2015**, *45*, 1345–1360. [CrossRef]
70. Woodhouse, S. Information Security: End User Behavior And Corporate Culture. In Proceedings of the 7th IEEE International Conference on Computer and Information Technology (CIT 2007), Aizu-Wakamatsu, Japan, 16–19 October 2007; pp. 767–774.
71. Franke, U.; Brynielsson, J. Cyber situational awareness–a systematic review of the literature. *Comput. Secur.* **2014**, *46*, 18–31. [CrossRef]
72. Reegu, F.; Khan, W.Z.; Daud, S.M.; Arshad, Q.; Armi, N. A rEliable Public Safety Framework For industrial internet of things (IIoT). In Proceedings of the 2020 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET), Tangerang, Indonesia, 18–20 November 2020; pp. 189–193.
73. Bajramovic, E.; Gupta, D.; Guo, Y.; Waedt, K.; Bajramovic, A. Security Challenges And Best Practices for IIoT. In Proceedings of the INFORMATIK 2019: 50 Jahre Gesellschaft fúr Informatik–Informatik fúr Gesellschaft (Workshop-Beitráge), Gesellschaft fúr Informatik eV, Vancouver, BC, Canada, 9–12 September 2019.
74. Conti, M.; Dargahi, T.; Dehghantanha, A. *Cyber Threat Intelligence: Challenges and Opportunities*; Springer: Berlin/Heidelberg, Germany, 2018.
75. Abu, M.S.; Selamat, S.R.; Ariffin, A.; Yusof, R. Cyber threat intelligence–issue and challenges. *Indones. J. Electr. Eng. Comput. Sci.* **2018**, *10*, 371–379.
76. Tounsi, W.; Rais, H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Comput. Secur.* **2018**, *72*, 212–233. [CrossRef]
77. Gao, P.; Shao, F.; Liu, X.; Xiao, X.; Liu, H.; Qin, Z.; Xu, F.; Mittal, P.; Kulkarni, S.R.; Song, D. A System for Efficiently Hunting For Cyber Threats In Computer Systems Using Threat Intelligence. In Proceedings of the 2021 IEEE 37th International Conference on Data Engineering (ICDE), Chania, Greece, 19–22 April 2021; pp. 2705–2708.
78. Barnum, S. Standardizing cyber threat intelligence information with the structured threat information expression (stix). *Mitre Corp.* **2012**, *11*, 1–22.
79. Merah, Y.; Kenaza, T. Ontology-based Cyber Risk Monitoring Using Cyber Threat Intelligence. In Proceedings of the 16th International Conference on Availability, Reliability and Security, Vienna, Austria, 17–20 August 2021; pp. 1–8.
80. Sadique, F.; Cheung, S.; Vakilinia, I.; Badsha, S.; Sengupta, S. Automated Structured Threat Information Expression (Stix) Document Generation With Privacy Preservation. In Proceedings of the 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 8–10 November 2018; pp. 847–853.
81. Yadav, T.; Rao, A.M. Technical aspects of cyber kill chain. In *Communications in Computer and Information Science, Proceedings of the Security in Computing and Communications: Third International Symposium, SSCC 2015, Kochi, India, 10–13 August 2015*; Proceedings 3; Springer: Berlin/Heidelberg, Germany, 2015; pp. 438–452.
82. Khan, M.S.; Siddiqui, S.; Ferens, K. A cognitive and concurrent cyber kill chain model. *Comput. Netw. Secur. Essent.* **2018**, 585–602.
83. Strom, B.E.; Applebaum, A.; Miller, D.P.; Nickels, K.C.; Pennington, A.G.; Thomas, C.B. *Mitre att&ck: Design and Philosophy*; Technical Report; The MITRE Corporation: McLean, VA, USA, 2018.
84. Al-Shaer, R.; Spring, J.M.; Christou, E. Learning the Associations of Mitre att & ck Adversarial Techniques. In Proceedings of the 2020 IEEE Conference on Communications and Network Security (CNS), Avignon, France, 29 June–1 July 2020; pp. 1–9.
85. Pols, P.; van den Berg, J. The Unified Kill Chain. CSA Thesis, Cyber Security Academy (CSA), The Hague, The Netherlands, 2017; pp. 1–104.
86. Firstbrook, P.; Lawson, C. *Innovation Insight for Extended Detection and Response*; Gartner ID G00718616; Gartner, Inc.: Stanford, CT, USA, 2021.
87. Caltagirone, S.; Pendergast, A.; Betz, C. *The Diamond Model Of Intrusion Analysis*; Technical report; Center For Cyber Intelligence Analysis and Threat Research: Hanover, MD, USA, 2013.
88. Irfan, A.N.; Chuprat, S.; Mahrin, M.N.; Ariffin, A. Taxonomy of Cyber Threat Intelligence Framework. In Proceedings of the 2022 13th International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Republic of Korea, 19–21 October 2022; pp. 1295–1300.
89. Bella, G.; Biondi, P.; Bognanni, S.; Esposito, S. PETIoT: PEnetration Testing the Internet of Things. *Internet Things* **2023**, *22*, 100707. [CrossRef]
90. Mwiki, H.; Dargahi, T.; Dehghantanha, A.; Choo, K.K.R. Analysis and triage of advanced hacking groups targeting western countries critical national infrastructure: Apt28, red october, and regin. In *Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies*; Springer: Cham, Switzerland, 2019; pp. 221–244.
91. Mei, Y.; Han, W.; Li, S.; Wu, X.; Lin, K.; Qi, Y. A Review of Attribution Technical for APT Attacks. In Proceedings of the 2022 7th IEEE International Conference on Data Science in Cyberspace (DSC), Guilin, China, 1–13 July 2022; pp. 512–518.
92. Vera, R.; Shehu, A.F.; Dargahi, T.; Dehghantanha, A. Cyber defence triage for multimedia data intelligence: Hellsing, Desert Falcons and Lotus Blossom APT campaigns as case studies. *Int. J. Multimed. Intell. Secur.* **2019**, *3*, 221–243. [CrossRef]
93. Solberg, I.C.; Høivik, M.L.; Cvancarova, M.; Moum, B. Risk matrix model for prediction of colectomy in a population-based study of ulcerative colitis patients (the IBSEN study). *Scand. J. Gastroenterol.* **2015**, *50*, 1456–1462. [CrossRef] [PubMed]

94. Huang, X.; Qiao, L. A risk index model for multi-period uncertain portfolio selection. *Inf. Sci.* **2012**, *217*, 108–116. [CrossRef]
95. Ho, C.T.B.; Wu, D.D.; Olson, D.L. A risk scoring model and application to measuring internet stock performance. *Int. J. Inf. Technol. Decis. Mak.* **2009**, *8*, 133–149. [CrossRef]
96. Yang, Z.; Zhang, Z. The Study on Resolutions of STRIDE Threat Model. In Proceedings of the 2007 First IEEE International Symposium on Information Technologies and Applications in Education, Kunming, China, 23–25 November 2007; pp. 271–273.
97. Li, P.; Yang, X.; Xiong, Q.; Wen, J.; Tang, Y.Y. Defending against the advanced persistent threat: An optimal control approach. *Secur. Commun. Netw.* **2018**, *2018*, 1–14. [CrossRef]
98. Yang, L.X.; Li, P.; Yang, X.; Tang, Y.Y. Security evaluation of the cyber networks under advanced persistent threats. *IEEE Access* **2017**, *5*, 20111–20123. [CrossRef]
99. Park, S.H.; Jung, J.W.; Lee, S.W. Multi-perspective APT Attack Risk Assessment Framework using Risk-Aware Problem Domain Ontology. In Proceedings of the 2021 IEEE 29th International Requirements Engineering Conference Workshops (REW), Notre Dame, IN, USA, 20–24 September 2021; pp. 400–405.
100. Fu, T.; Lu, Y.; Zhen, W. APT attack situation assessment model based on optimized BP neural network. In Proceedings of the 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chengdu, China, 15–17 March 2019; pp. 2108–2111.
101. Li, S.; Zhang, Q.; Wu, X.; Han, W.; Tian, Z. Attribution classification method of APT malware in IoT using machine learning techniques. *Secur. Commun. Netw.* **2021**, *2021*, 1–12. [CrossRef]
102. Do Xuan, C. Detecting APT attacks based on network traffic using machine learning. *J. Web Eng.* **2021**, 171–190. [CrossRef]
103. Wang, X.; Liu, Q.; Pan, Z.; Pang, G. APT attack detection algorithm based on spatio-temporal association analysis in industrial network. *J. Ambient. Intell. Humaniz. Comput.* **2020**, 1–10. https://orcid.org/10.1007/s12652-020-01840-3. [CrossRef]
104. Moon, D.; Im, H.; Kim, I.; Park, J.H. DTB-IDS: An intrusion detection system based on decision tree using behavior analysis for preventing APT attacks. *J. Supercomput.* **2017**, *73*, 2881–2895. [CrossRef]
105. Zhang, R.; Huo, Y.; Liu, J.; Weng, F. Constructing APT attack scenarios based on intrusion kill chain and fuzzy clustering. *Secur. Commun. Netw.* **2017**, *2017*, 7536381. [CrossRef]
106. Schindler, T. Anomaly detection in log data using graph databases and machine learning to defend advanced persistent threats. *arXiv* **2018**, arXiv:1802.00259.
107. Breslau, L.; Estrin, D.; Fall, K.; Floyd, S.; Heidemann, J.; Helmy, A.; Huang, P.; McCanne, S.; Varadhan, K.; Xu, Y.; et al. Advances in network simulation. *Computer* **2000**, *33*, 59–67. [CrossRef]
108. Wehrle, K.; Gúnes, M.; Gross, J. *Modeling and Tools for Network Simulation*; Springer Science & Business Media: Berlin, Germany, 2010.
109. Siraj, S.; Gupta, A.; Badgujar, R. Network simulation tools survey. *Int. J. Adv. Res. Comput. Commun. Eng.* **2012**, *1*, 199–206.
110. Yoon, S.; Kim, Y.B. A design of network simulation environment using ssfnet. In Proceedings of the 2009 First International Conference on Advances in System Simulation, Porto, Portugal, 20–25 September 2009; pp. 73–78.
111. Kim, J.; Kim, H.J. Poster: Modeling of APT Attacks through Transforming Attack Scenarios into DEVS Models. *IEEE Secur. Priv.* **2015**.
112. Lu, S.S.; Wang, X.F.; Mao, L. Network security situation awareness based on network simulation. In Proceedings of the 2014 IEEE Workshop on Electronics, Computer and Applications, Ottawa, ON, USA, 8–9 May 2014; pp. 512–517.
113. Gultom, R.A.; Alrianto, B. Enhancing network security environment by empowering modeling and simulation strategy. In Proceedings of the Eleventh International Conference on Internet Monitoring and Protection Enhancing, Valencia, Spain, 22–26 May 2016; pp. 45–52.
114. Morato, D.; Pérez-Gómara, C.; Magaña, E.; Izal, M. Network simulation in a TCP-enabled industrial internet of things environment-reproducibility issues for performance evaluation. *IEEE Trans. Ind. Inform.* **2022**, *18*, 807–815. [CrossRef]
115. Rajaram, M.L.; Kougianos, E.; Mohanty, S.P.; Choppali, U. Wireless sensor network simulation frameworks: A tutorial review: MATLAB/Simulink bests the rest. *IEEE Consum. Electron. Mag.* **2016**, *5*, 63–69. [CrossRef]
116. Li, Y.; Huang, G.Q.; Wang, C.Z.; Li, Y.C. Analysis framework of network security situational awareness and comparison of implementation methods. *EURASIP J. Wirel. Commun. Netw.* **2019**, *2019*, 1–32. [CrossRef]
117. Rife, R.H.B.H. Improving Information Security Awareness Training Through Real-Time Simulation Augmentation. Ph.D. Thesis, Northcentral University, Scottsdale, AZ, USA, 2019.
118. Khalid, A.; Zainal, A.; Maarof, M.A.; Ghaleb, F.A. Advanced Persistent Threat Detection: A Survey. In Proceedings of the 2021 3rd International Cyber Resilience Conference (CRC), Langkawi Island, Malaysia, 29–31 January 2021; pp. 1–6.
119. Shah, Y.; Sengupta, S. A survey on Classification of Cyber-attacks on IoT and IIoT devices. In Proceedings of the 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 28–31 October 2020; pp. 0406–0413.
120. Alruwaili, F.F. Intrusion Detection and Prevention in Industrial IoT: A Technological Survey. In Proceedings of the 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Mauritius, 7–8 October 2021; pp. 1–5.
121. Quintero-Bonilla, S.; del Rey, M. A New Proposal on the Advanced Persistent Threat: A Survey. *Appl. Sci.* **2020**, *10*, 3874 [CrossRef]

122. Mei, Y.; Han, W.; Li, S.; Wu, X. A Survey of Advanced Persistent Threats Attack and Defense. In Proceedings of the 2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC), Shenzhen, China, 9–11 October 2021; pp. 608–613.
123. Sengupta, J.; Ruj, S.; Bit, S. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. *J. Netw. Comput. Appl.* **2020**, *149*, 102481. [CrossRef]
124. Boyes, H.; Hallaq, B.; Cunningham, J.; Watson, T. The industrial internet of things (IIoT): An analysis framework. *Comput. Ind.* **2018**, *101*, 1–12. [CrossRef]
125. Ning, H.; Wang, Z. Future internet of things architecture: Like mankind neural system or social organization framework? *IEEE Commun. Lett.* **2011**, *15*, 461–463. [CrossRef]
126. Olivier, F.; Carlos, G.; Florent, N. New security architecture for IoT network. *Procedia Comput. Sci.* **2015**, *52*, 1028–1033. [CrossRef]
127. Biswas, K.; Muthukkumarasamy, V.; Wu, X.W.; Singh, K. Performance evaluation of block ciphers for wireless sensor networks. In *Advances in Intelligent Systems and Computing, Proceedings of the Advanced Computing and Communication Technologies: Proceedings of the 9th ICACCT*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 443–452.
128. Guo, X.; Hua, J.; Zhang, Y.; Wang, D. A complexity-reduced block encryption algorithm suitable for internet of things. *IEEE Access* **2019**, *7*, 54760–54769. [CrossRef]
129. Malik, M.; Dutta, M.; Granjal, J. A survey of key bootstrapping protocols based on public key cryptography in the Internet of Things. *IEEE Access* **2019**, *7*, 27443–27464. [CrossRef]
130. Fun, T.S.; Samsudin, A. Attribute based encryption—A data centric approach for securing internet of things (IoT). *Adv. Sci. Lett.* **2017**, *23*, 4219–4223. [CrossRef]
131. Mosteiro-Sanchez, A.; Barcelo, M.; Astorga, J.; Urbieta, A. Securing IIoT using defence-in-depth: Towards an end-to-end secure industry 4.0. *J. Manuf. Syst.* **2020**, *57*, 367–378. [CrossRef]
132. Bader, J.; Michala, A.L. Searchable encryption with access control in industrial internet of things (IIoT). *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 1–10. [CrossRef]
133. Nunes, E.; Diab, A.; Gunn, A.; Marin, E.; Mishra, V.; Paliath, V.; Robertson, J.; Shakarian, J.; Thart, A.; Shakarian, P. Darknet and deepnet mining for proactive cybersecurity threat intelligence. In Proceedings of the 2016 IEEE Conference on Intelligence and Security Informatics (ISI), Tucson, AZ, USA, 28–30 September 2016; pp. 7–12.
134. Almukaynizi, M.; Nunes, E.; Dharaiya, K.; Senguttuvan, M.; Shakarian, J.; Shakarian, P. Proactive identification of exploits in the wild through vulnerability mentions online. In Proceedings of the 2017 International Conference on Cyber Conflict (CyCon US), Washington, DC, USA, 7–8 November 2017; pp. 82–88.
135. Benjamin, V.; Li, W.; Holt, T.; Chen, H. Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops. In Proceedings of the 2015 IEEE international conference on intelligence and security informatics (ISI), Baltimore, MD, USA, 27–29 May 2015; pp. 85–90.


**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.