Review

Not peer-reviewed version

A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-based Solutions, and Edge Computing Opportunities

Bandar Alotaibi *

Posted Date: 12 July 2023

doi: 10.20944/preprints202307.0771.v1

Keywords: internet of things; fog computing; edge computing; industrial internet of things; industry 4.0; cyber-physical systems; cybersecurity

Article

A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions, and Edge Computing Opportunities

Bandar Alotaibi

Department of Information Technology, University of Tabuk, Tabuk 47731, Saudi Arabia; b-alotaibi@ut.edu.sa

Abstract: The Industrial Internet of Things (IIoT) paradigm is a key research area derived from the Internet of Things (IoT). The emergence of IIoT has enabled a revolution in manufacturing and production, through the employment of various embedded sensing devices connected with each other by an IoT network, along with a collection of enabling technologies such as artificial intelligence (AI) and edge/fog computing. One of the unrivaled characteristics of IIoT is the inter-connectivity provided to industries; however, this characteristic might open the door for cyber-criminals to launch various attacks. In fact, one of the major challenges hindering the prevalent adoption of the IIoT paradigm is IoT security. Inevitably, an increasing number of research proposals have been introduced over the last decade to overcome these security concerns. To obtain an overview of this research area, conducting a literature survey of the published research is necessary, eliciting the various security requirements and their considerations. This paper provides a literature survey of IIoT security, focused on the period from 2017 to 2023. We identify IIoT security threats and classify them into three categories, based on the IIoT layer they exploit to launch these attacks. Additionally, we characterize the security requirements that these attacks violate. Finally, we highlight how emerging technologies, such as AI and edge/fog computing, can be adopted to address security concerns and enhance IIoT security.

Keywords: internet of things; fog computing; edge computing; industrial internet of things; industry 4.0; cyber-physical systems; cybersecurity

1. Introduction

The Internet of Things (IoT) can be defined as a paradigm that utilizes intelligent devices which can communicate with each other through the Internet [1,2]. IoT environments comprise many intelligent devices capable of collecting, processing, transmitting, and receiving data from each other [3]. These interconnected intelligent devices help us to monitor any environment and precisely control any setting [4]. By 2025, the total economic impact derived from IoT technology annually has been predicted to reach $11.1 trillion [5]. As most of the IoT systems developed so far are consumer-centric, their nature has enabled the adoption of this technology in many industrial applications, creating the so-called IIoT technology [6]. IIoT, also known as industrial Internet, can be defined as a paradigm that utilizes interconnected intelligent devices deployed in an industrial environment, in order to connect industrial components, including actuators, sensors, controllers, and intelligent control systems (i.e., for data analysis and industrial process optimization to enhance the speed of execution, decrease costs, and manage the industrial setting dynamically) [7].

As shown in Figure 1, Industry 4.0—also known as the fourth industrial revolution—exemplifies an unprecedented industrial evolution and complements various emerging technologies and systems, such as CPS, MCC, IoT, AI, CC, and fog computing, in order to improve the adequacy of industries, in terms of heterogeneous data support, automation, high production, and integrating knowledge [8,9]. The number of embedded systems utilized in industrial applications has grown swiftly, due to the mounting availability, capability, and affordability of sensors, communication modules, and processes [10]. This has driven more interest regarding the use of IIoT in industrial domains such

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 July 2023 doi:10.20944/preprints202307.0771.v1

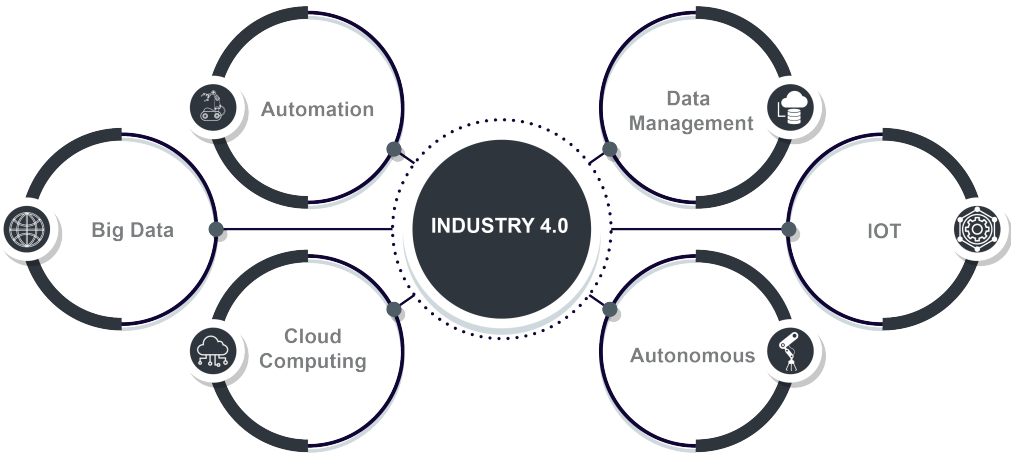

Figure 1. Industry 4.0 utilizes various emerging technologies to improve industrial production.

as smart cities, transportation, healthcare, micro-grids, and smart factory, giving rise to Industry 4.0 based on CPS. By 2030, IIoT has been forecasted to be worth $7.1 trillion in the U.S. and to exceed $1.2 trillion in European countries [11].

Despite all of the advantages of adopting IIoT, IoT security issues represent one of the biggest challenges hindering its perfect utilization. The poor security associated with IoT devices [12,13] makes them vulnerable to cyber-attacks (e.g., IoT devices could be targeted by adversaries to execute devastating attacks, such as DDoS) [14]. Thus, they may be susceptible to various cybersecurity threats, causing IIoT security to become a hot topic in recent years [15]. IoT also relies heavily on the CC to provide the IoT devices with limited capabilities for the desired services [16]; however, this dependency transports diverse vulnerabilities to IoT environments [17].

In this context, an emerging computing technology, known as fog computing, has attracted the attention of the research community [18]. Fog computing is a new paradigm that bridges the gap between CC and IoT by diffusing services and resources on the path between IoT environments and CC [19]. Fog computing has several advantages, which can facilitate the secure deployment of IIoT devices. However, fog computing may also bring some inherited security challenges to the table [20]. This paper investigates the security challenges associated with integrating IIoT and AI, edge/fog computing, and the solutions to several security issues that AI and edge/fog computing might bring to IIoT environments.

The contributions of this paper can be summarized as follows:

- The security advantages of integrating AI and edge/fog computing with IIoT are explored.
- The security requirements and challenges encountered in IIoT environments are highlighted.
- Solutions based on AI and edge/fog computing to these security challenges are thoroughly investigated.

Section 2 introduces the research methodology followed to write this survey. Section 3 presents the background of IIoT and edge/fog computing. Section 4 compares the research in this paper with the related literature. Section 5 discusses the security requirements that should be satisfied by IIoT environments. Section 6 presents the attacks that target each layer of the IIoT paradigm reference architecture. Section 7 introduces the state-of-the-art solutions proposed to provide secure deployment of IIoT devices on edge computing. Section 8 presents the opportunities provided by edge/fog computing to IIoT environments, the challenges that IIoT environments face, and the future research directions. Section 9 concludes the survey paper.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 July 2023 doi:10.20944/preprints202307.0771.v1

2. Research Methodology

This survey paper utilizes a profound valuation blueprint for exemplary survey structure. This paper concentrates on the security requirements for IIoT environments, investigate possible attacks targeting these environments, explores security solutions that protect IIoT environments from these attacks, highlights opportunities provided by edge computing, and introduces future directions. We followed a quantitive approach to search for ideas regarding each one of these concentrations. However, we try to focus more on the last six years. The information is collected from various sources such as journal articles, conference papers, book chapters, and online sources. The collection sources include publication houses and public databases such as ScienceDirect, IEEE Xplore, Springer, MDPI, arxiv (i.e., e-Print archive), Hindawi, and Researchgate. Various keywords related to the topic of the survey paper were employed to search for the state-of-art articles in these databases. Many articles were returned, but we carefully chose 231 articles to write this survey paper, as shown in Figure 2. Twenty papers were used to write the introduction section. Eleven papers were used to write the IoT/IIoT background and Edge/Fog computing background. Seventeen closely related papers were precisely compared with our survey. The security requirements section was written utilizing forty-one papers. Sixty-one papers were employed in the attack categories section. The security solutions section was written using fifty papers, in which 27 papers were utilized to write the network layer security solutions subsection, eight papers were used to write the perception layer security solutions subsection, and 15 papers were employed to write the application layer security solutions subsection. Finally, thirty-one references were used to write the opportunities and future directions section.

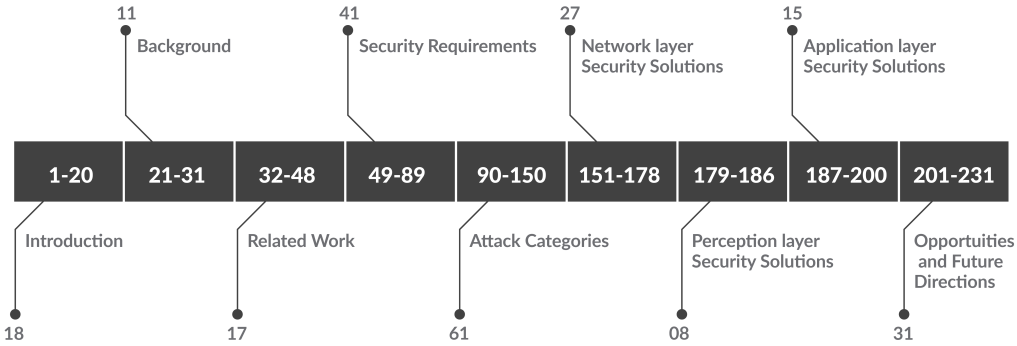

Figure 2. These papers (i.e., 231 articles) were carefully chosen to write this survey paper.

3. IoT/IIoT and Edge/Fog Computing Background

This section is divided into two subsections: Subsection 3.1 presents the concepts of IoT and its IIoT subset, while subsection 3.2 introduces two CC extensions (i.e., edge and fog computing).

3.1. IoT and IIoT

Although IIoT originated from IoT it has different focuses, in terms of practical applications and concepts [21], as shown in Table 1. Namely, the IoT has been designed to improve people's quality of life and is generally considered consumption-centric. Typical IoT application examples include health monitoring, indoor localization, and smart homes [22]. On the other hand, the IIoT endeavors to enhance the production efficiency of industries (i.e., it is considered a production-centric paradigm). Typical IIoT applications include smart manufacturing, smart transportation, remote maintenance, and intelligent logistics [23]. IoT application system frameworks are generally constructed from scratch, and the utilized sensors are deployed within a small area and are not sensitive to precision [6]. High mobility is one of the main characteristics of IoT devices; the generated data of these devices are of moderate size, and delays can be tolerated to a great extent. Meanwhile, IIoT application system frameworks rely on traditional industrial infrastructures. Thus, the sensors are typically distributed

 doi:10.20944/preprints202307.0771.v1

over a large area, and the deployment must be highly precise. Conversely, most IIoT devices are distributed in specific locations; the data generated by these devices are large in size, and only slight delays can be tolerated.

Table 1. Comparison of main characteristics of IoT and IIoT.

Characteristic	IoT	IIoT
Application examples	Smart home, health monitoring, indoor localization	Smart transportation, intelligent logistics, smart manufacturing, remote maintenance
System Framework	Self-reliant	Industrial facility-reliant
Delay sensitivity	High	Low
Mobility	High	Low
Deployment size	Small	Large
Deployment preciseness	Low	High
Data volume	Medium	High

The IoT terminology relates to other famous concepts, such as CPS, Industry 4.0, and Industrial Internet. The CPS concept, introduced in 2006 by Helen Gill, involves the thorough integration of several technologies, such as sensing and embedded systems (i.e., combining software and hardware), in order to accomplish efficient internal information exchange, resilient real-time feedback, and positive communication between virtual and physical entities [24]. IoT is regarded as a subset of CPS, which assures communication between diverse objects through the Internet, depending on unique identifiers. The IoT is supported by the Internet, which provides the IoT devices with availability, interoperability, universality, and socialization [25]. Another concept, introduced by the IIC and initiated by five U.S. tech companies (i.e., Cisco, Intel, IBM, AT&T, and GE) is Industrial Internet, which concentrates on data flow enhancement, innovative network standardization, application, construction, and industrial field automated transformation.

Industry 4.0 was introduced in Germany. This global concept utilizes CPS and emerging technologies, such as AI, IoT (i.e., forming the IIoT idea), big data, and CC, in intelligent manufacturers [26]. To recap, CPS connects objects to link the virtual and physical worlds, while IoT utilizes physical addresses in civilian and industrial settings to facilitate communication between objects. The industrial Internet uses emerging technologies to depict the prospect of future trends. In this context, industrial Internet and IoT are considered subsets of CPS [27,28], and intersect to form the so-called IIoT. Moreover, Industry 4.0 utilizes IIoT, among other emerging technologies, in intelligent manufacturing settings. Figure 3 depicts the relationships existing between the concepts introduced in this subsection.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 July 2023 doi:10.20944/preprints202307.0771.v1

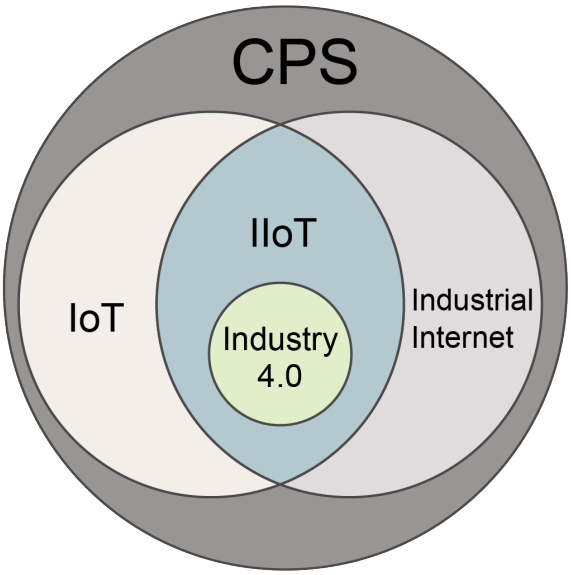

Figure 3. The relationships between CPS, IoT, IIoT, Industrial Internet, and Industry 4.0.

3.2. Edge and Fog Computing

Edge computing is an enabling paradigm that exclusively processes data on the network's edge. This occurs between centralized cloud servers and end devices (e.g., sensors, actuators, and controllers). One of the main reasons for initiating edge computing is to bring computations closer to hosts, thus reducing delays. Therefore, edge computing enables data to be transferred from end devices to edge computing (i.e., close to end devices) and vice versa, instead of imposing that the end devices interact with cloud servers. Thus, as shown in Figure 4, edge platforms can act as clients and servers; namely, clients to cloud servers, and servers to end devices. Acting as servers, they enable end-devices to gain the full benefits from edge platforms that can carry out caching, computational off-loading, storage capabilities, and processing [29].

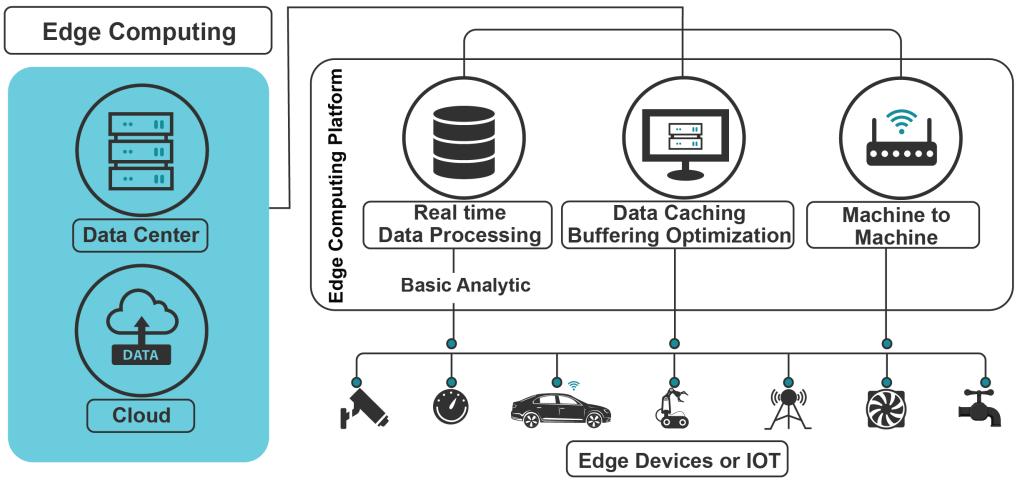

Figure 4. The interaction between edge platforms and the upper layer (cloud servers) and the lower layer (edge devices).

Fog computing is another emerging technology that enables edge devices (i.e., end devices and edge platforms) to perform additional computations, handle data, and allocate network resources [30].

 doi:10.20944/preprints202307.0771.v1

Thus, fog computing is not far from the end-devices and enables the end-devices/edge platforms to carry out most services (e.g., data handling, storage, network resources utilization, and processing) that cloud services can afford [31]. Therefore, edge and fog computing enable delay-sensitive end-device applications to carry out various services in real-time. These two emerging technologies have become a viable supplement to CPS and applications in IIoT environments. The following requirements are satisfied by edge and fog computing:

1. **System performance enhancement:** Data processing can be achieved at the network's edge, improving the system performance of end devices. Edge platforms can accomplish data processing in milliseconds, reducing the latency and communication bandwidth demand, thus enhancing the system's performance.
2. **Data security and privacy protection:** Edge and fog computing can reduce privacy and security risks, as they transmit and store data in decentralized devices (i.e., near-end devices), as opposed to cloud platforms, which provide centralized data protection solutions. Additionally, data leakage at centralized cloud servers affects many end devices, compared to data leakage at edge/fog devices, involving only a limited number of devices (i.e., the end devices nearby that obtain services from edge/fog platforms).
3. **Operational cost reduction:** When end devices transfer data directly to the cloud, the operational costs related to migrating data, maintaining good bandwidth, and shortening delays are increased. On the other hand, when edge/fog platforms are utilized, the data migration volume, delay, and bandwidth consumption are decreased, leading to reduced operational costs.

4. Related Work

In this section, we detail recent survey papers that are closely related to this review, including the state-of-the-art in IoT security, IIoT security, edge computing security, and edge computing in IIoT, as shown in Table 2. Thus, there is a need to survey the secure deployment of edge/fog computing in IIoT environments.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 July 2023 doi:10.20944/preprints202307.0771.v1

Table 2. Comparison of the related literature.

Scope	Ref.	Major contribution	Advantages	Limitations
IoT security	[32]	A comprehensive overview of IIoT security threats	Attacks perfectly linked to security requirements	The role of emerging technologies in securing IoT networks is not discussed
	[33]	A detailed review of IoT threats and vulnerabilities	A distinctive categorization of IoT vulnerabilities and a discussion of about 100 research ideas	Attacks are not completely linked to security requirements and the impact of integrating emerging technologies on IoT security are not discussed
	[34]	An overview of security requirements for several IoT application domains	Noteworthy security requirement prioritization for each application domain	The depth of the challenges section is minimal
IIoT security	[35]	A comprehensive review of cyberattack classes	Outstanding future directions and potential applications are discussed	Cyberattacks are not linked to security requirements and the impact of emerging technologies on IIoT security is not discussed
	[6]	A survey of challenges faced by Industry 4.0 environments	A unique overview of challenges related to energy adequacy, interoperability, and security	Security requirements and emerging technologies impact are not discussed
	[36]	An overview of IIoT security solutions	A unique description of the building and linking of IIoT devices with security in mind	The depth of the survey is minimal
	[37]	A unified architecture format of security requirements in IIoT	A detailed comparison of security requirements within heterogeneous IIoT devices	The authors discuss a limited number of use cases
	[38,39]	A discussion of IIoT security requirements	A comprehensive overview of solutions that deal with security violations	The depth of the review is minimal
	[40]	An overview of IIoT security, threats, and counter-measures taken by industries	A distinctive categorization of the IIoT, exploration of counter-measures taken by industries utilizing security requirements	Lacks discussion of the role of adopting emerging technologies to protect the IIoT paradigm

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 July 2023 doi:10.20944/preprints202307.0771.v1

Table 2. *Cont.*

Scope	Ref.	Major contribution	Advantages	Limitations
Edge security	[41]	A overview of edge-IoT paradigm and applications	An investigation of opportunities provided by edge computing to improve IIoT security	The depth of the overview is minimal
	[42]	A thorough discussion of fog computing security and privacy issues	A distinctive observation related to the unsuitability of methods used to secure CC for fog computing is introduced	The depth of the discussion is minimal
	[43]	A detailed tutorial of the edge computing paradigm	Incandescent solutions to privacy and security are thoroughly discussed	The connection between edge applications, threats targeting them, and security solutions is missing
Edge Computing in IIoT	[44]	A roadmap for smart manufacturing to integrate IoT and edge computing	One of the first surveys to discuss this area	Security requirements and challenges are inadequately discussed
	[45]	A demonstration of two scenarios of how IIoT benefits from fog computing	A unique comparison of cloud and fog computing when integrated with IIoT	The overview is scenario-specific (i.e., not comprehensive)
	[46]	An overview of edge computing reference architectures in IIoT	A comparison of reference architectures is presented	The depth of this overview is minimal
	[47]	A discussion of the integration of fog computing and IIoT	Two enabling technologies that can add value to the integration are uniquely discussed	This survey is not comprehensive
	[48]	A review of edge computing and IIoT integration	A discussion of recently proposed solutions, recent challenges and few use-cases	The lack of in-depth discussion of security challenges and sufficient application examples
	[8]	Discussion of the industrial revolution background and transformation enabling technologies	A well-organized and thorough discussion of communication and network protocols	The discussion part of edge computing lacks essential details
	[21]	A review of current solutions related to adopting edge computing into IIoT	Distinctive technical details of some significant edge services that add value to the IIoT paradigm	Security opportunities brought when integrating edge computing into IIoT is partially discussed

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 July 2023 doi:10.20944/preprints202307.0771.v1

Table 2. *Cont.*

Scope	Ref.	Major contribution	Advantages	Limitations
Secure IIoT-Edge	[10]	A systematic survey of IIoT security over the period of 2011–2019	A thorough discussion of IIoT security challenges, requirements, and opportunities provided when adopting edge computing that could secure IIoT paradigm	The IIoT attacks are not deeply discussed and the depth of the opportunities part is not sufficient
	Ours	A thorough categorization of IIoT attacks, security requirements, and security benefits from integrating edge computing and IIoT	A distinctive linkage of IIoT attacks and requirements is introduced and research attempts to overcome security challenges (with a focus on the period 2019–2022) are comprehensively discussed	N/A

 doi:10.20944/preprints202307.0771.v1

4.1. IoT Security Surveys

Meneghello *et al.* [32] have classified IoT attacks into different categories. The authors defined various security requirements for IoT environments, including access control, integrity, privacy, anonymity, authorization, authentication, and resilience, and linked various attacks to suggested security requirements in a well-planned manner. However, this paper lacked a discussion of the role of emerging technologies, such as edge/fog computing and AI, in securing IoT networks. Neshenko *et al.* [33] have conducted a detailed survey and provided a distinctive classification of IoT attacks and vulnerabilities. The authors also broadly discussed research contributions advancing the state-of-the-art; however, these attacks were not linked to security requirements. Famous threats associated to IoT devices discussed by the authors, such as improper patch management, false data injection, and lack of encryption, can be easily linked to security requirements. Furthermore, the authors did not discuss the positive impact of integrating emerging technologies on IoT security.

Kouicem *et al.* [34] have presented an IoT security survey utilizing a top-down approach. The authors explored the security requirements in various IoT application domains, such as smart transportation, healthcare, smart homes, smart grids, and smart cities. Some of the discussed application domains, such as smart transportation, can play a part in the IIoT paradigm. The authors also identified specific security requirements for each application domain. For instance, they defined five security requirements for smart grids: Confidentiality, availability, integrity, privacy, and accountability. In addition, the authors defined some challenges related to IoT devices and networks, such as heterogeneity, privacy, and scalability. It appears that the priority of the security requirements in each application domain differed; for example, confidentiality and privacy are considered more important for healthcare than smart transportation. A significant observation introduced in this survey is revealing a security requirement that might be more crucial to IIoT environments, compared to traditional IoT environments, which is related to safety in IIoT environments (e.g., plants). One drawback of this survey is its lack of depth in some sections, such as the challenges part.

4.2. IIoT Security Surveys

Lezzi *et al.* [35] have classified IIoT cyberattacks into different categories, while Sisinni *et al.* [6] have investigated the challenges encountered in Industry 4.0 environments, as well as discussing the distinction between operational and information technology in these environments. Neither of the above-mentioned surveys investigated the security requirements in the IIoT paradigm or deeply discussed the effectiveness of adopting emerging technologies to enhance the security of IIoT environments.

Hofer [36] has noted the growth of articles focusing on IIoT security and discussed some of these articles. However, the depth of the security discussion was minimal. Hansch *et al.* [37] have defined the security requirements in IIoT open-platform communications, and organized them in a unified architecture format. The authors discussed the security requirements well but did not discuss enough use cases. Other previous reviews [38,39] have discussed IIoT security solutions and explored security requirements for the IIoT paradigm. These surveys lacked discussions of the existing security solutions and requirements in depth, however.

Tan and Samsudin [40] have introduced a detailed survey of IIoT security, discussed the counter-measures taken by industries to protect their perimeters, discussed current challenges, and suggested future directions for research. The authors categorized the IIoT paradigm into four layers and inspected the countermeasures deployed by industries utilizing the security requirements presented in the CIA+ security certification. One drawback of this survey was a lack of discussion regarding the role of adopting emerging technologies to secure IIoT environments and related use cases.

 doi:10.20944/preprints202307.0771.v1

4.3. Edge Computing Security Surveys

Ni *et al.* [41] have presented a complete edge-IoT paradigm and discussed various emerging edge-based IoT applications. The authors investigated mobile edge computing data processing challenges related to privacy, security, and efficiency. Additionally, the authors explored some opportunities, such as secure data de-duplication, secure data aggregation, and secure computational offloading, provided by edge computing that could enhance the computational efficiency of IoT data security. The authors also introduced various motivating future research directions related to data analysis at the edge of networks.

Guan *et al.* [42] have discussed fog computing-related privacy and data security issues. The authors surveyed fog layer security design challenges and also argued that data protection methods used to secure cloud computing are not directly suitable for fog computing. Zhang *et al.* [43] have provided a comprehensive tutorial on edge computing architectures. The authors also discussed edge computing privacy and data security requirements, mechanisms, and challenges. Additionally, the authors suggested various future directions to effectively secure edge computing technology.

4.4. Edge Computing in IIoT Surveys

Some reviews have covered the integration of edge computing and IIoT in part. For example, Georgakopoulos *et al.* [44] have presented a roadmap for smart manufacturing to efficiently utilize IoT and edge computing. Seitz *et al.* [45] have introduced two empirical scenarios, in order to demonstrate that IIoT applications can benefit from fog computing. The first practical scenario explains how the fog computing paradigm increases the system availability, compared to cloud computing, and demonstrates how the sensor data can be analyzed in fog computing with a low delay, compared to cloud computing. The second practical scenario is implemented in an industry setting, which indicates a decrease in bandwidth utilization, allowing for the deployment issues associated with cloud computing to be overcome and lead to reliable and efficient IIoT applications. Sitton *et al.* [46] have explained the major state-of-the-art edge computing reference paradigms in Industry 4.0, and compared and contrasted these reference architectures. Steiner and Poledna [47] have discussed how fog computing could be integrated with IIoT in an architectural manner, and explored two enabling technologies that can perfectly work with fog computing (i.e., deterministic communication and virtualization). Although these surveys introduced valuable knowledge with respect to integrating IIoT and edge computing, they were not comprehensive.

Other surveys have discussed the various main topics related to integrating IIoT and edge computing; however, the depth of these surveys remains low. For instance, Aazam *et al.* [48] have explained how fog computing adds value to IIoT environments, discussed some research challenges, and presented a few use-cases; however, they did not discuss the emerging technologies that could enhance the efficiency and secrecy of IIoT environments when integrated with edge computing. Furthermore, the survey paper lacked an in-depth discussion of challenges (security challenges in particular) and sufficient application examples. Basir *et al.* [8] have discussed the industrial revolution background and key technologies facilitating industrial transformation. The authors also discussed some challenges related to fog computing. However, their survey was highly concentrated on the communication and network protocols/algorithms used in IIoT, instead of focusing on the challenges associated with adopting edge computing.

Qiu *et al.* [21] have reviewed research articles related to edge computing in IIoT. The authors first discussed the background of edge computing and IIoT in detail. Then, they introduced the edge computing research progress and proposed a prospective edge computing architecture, including technical details such as task scheduling, data storage, routing, security, analytics, and standardization, that could be adopted by IIoT environments. Moreover, the authors discussed the opportunities that edge computing can afford in IIoT environments, such as data security, load balancing, data off-loading, and intelligence. They also discussed some challenges concerning the adoption of edge computing into IIoT environments and presented various application scenarios, such as smart grids,

 doi:10.20944/preprints202307.0771.v1

smart manufacturing, smart logistics, and ICV. However, the authors only partially discussed security aspects.

4.5. Secure IIoT-Edge Deployment

Tange *et al.* [10] have provided a systemic review of IIoT security over the period 2011–2019. The authors concentrated on the security requirements of IIoT and pointed out briefly how fog computing can enhance IIoT security. Although the authors pointed out some security benefits that might be introduced when adopting edge computing in IIoT environments, the depth of the security part when adopting edge computing in IIoT environments was insufficient, and the security challenges and the research progress required to overcome these security challenges were not deeply discussed in this survey. To fill this gap, a survey focused on the security challenges introduced when IIoT environments integrate edge computing, and the research attempts to overcome these security challenges are discussed in this survey paper.

5. IIoT Security Requirements

In this section, we introduce the general security requirements that should be satisfied by each communication system, including IIoT environments when deploying IIoT devices for edge computing.

5.1. CIA Triad

The famous information security model known as the CIA triad can be regarded as a building block for security requirements or goals. A set of security mechanisms also belong to these three requirements, briefly defined as follows:

- Confidentiality concerns the protection of information in any form. The methods used to satisfy confidentially include access control, encryption, network isolation, and privacy.
- Integrity aims to provide IIoT entities with consistency, authenticity, and accuracy, and allows for building trust with other entities.
- Availability guarantees that the system operates efficiently at all times. Various methods are used to satisfy availability, such as decentralization and redundancy.

Traditionally, the CIA model was utilized in the information security field, implying that this model is exclusively linked to information. Nevertheless, the CIA model is evenly adaptable in other fields, including CPS [49]. Conventionally, industrial environments concentrate primarily on availability, then on integrity, and finally on confidentiality. Meanwhile, with the use of Internet-connected devices, this conception should be re-considered, such that all three requirements should be treated equally. Therefore, with the evolution of Industry 4.0 and the IIoT paradigm, integrity and confidentiality must be considered evenly, with respect to availability.

While the CIA security model provides a good foundation and remains of paramount importance when security requirements are specified for a certain system, it is not always valuable for reducing solid requirements back to elements of this security model, if one already has more (e.g., contextual) information that might enable the derivation of a specific security requirement. For instance, we could simply declare that we should keep data confidential at rest; however, such a security goal might not imply the states that should be met by a specific confidentiality mechanism. Furthermore, this is open to interpretation. For example, which party should have their information kept confidential? It is difficult to design a constant security goal that works well in all scenarios [10].

5.2. Authentication

A major concern in various communication environments, such as IIoT, is authenticating remote entities (e.g., machines, users, and applications) [50]. In the context of IIoT applications, authentication becomes more challenging, due to the nature of IIoT devices, which have limited capabilities due to power constraints, as well as limited storage and processing capacities [51]. Thus, a lightweight

 doi:10.20944/preprints202307.0771.v1

authentication mechanism with features such as light computation overhead and minimum transfer size should be designed to overcome these limitations.

Another significant concern related to data authenticity is whether data integrity is verifiable and that they are not altered in transit [52]. Additionally, this applies to configuration files, which should be verified to have been created by authorized entities and not altered since their creation. Considering the nature of IIoT devices, IIoT environments require authentication solutions that satisfy the trade-off between lightweight and secrecy, as well-known authentication mechanisms will not be able to be adopted in such environments [53].

5.3. Access Control and Authorization

Access control is significant in various circumstances. Devices in IIoT environments should be given permission to access edge network resources, based on their privileges. For instance, system administrators would be given more permissions (e.g., for updates deployment) than normal users. In some situations, IIoT devices run on two operation modes: an administrator and a normal user. In this context, adequately separating privileges is one of the biggest challenges that systems (e.g., SCADA) in IIoT environments encounter [54]. On the other hand, unauthorized users should be prevented from accessing sensitive data or altering data [55].

Access control is usually regarded to be authentication-reliant, as it is necessary to authenticate users before access policy enforcement. Thus, access control mechanisms are typically similar to authentication mechanisms. Access control can consume IIoT device resources, as the IIoT devices must interact with authorization servers on the edge before they can access certain resources. Access control is somehow affected by availability, especially in the IIoT environment (i.e., it is highly distributed); thus, access control policies should be available to IIoT devices at all times.

5.4. Resilience and Maintainability

Resilience is defined by ICS in its IIoT security framework as an emerging mechanism equipped with a system that normally carries out the assigned missions, even if it encounters adversarial conditions. This system must avoid, absorb, and coordinate dynamically to work properly and complete its designated tasks. Once the system is infected, it should be capable of reconstituting its operational capabilities. This terminology is similar in concept to other security terminologies, such as reliability, safety, and trustworthiness [56]. Resilience is one of the most significant security challenges in IIoT environments [57].

IIoT networks should provide some mechanisms to guarantee that operations on IIoT systems will be normally performed, even if a part of the system is compromised. This could be done in IIoT networks by forwarding some of the current tasks from the infected part to another part of the system, or even to a different system. In the research community, this technique is usually called diversity, redundancy, or hardening [58]. This concept is applicable in WSNs, in which a sufficient number of sensors are deployed to ensure redundancy. Such a scenario aims to isolate compromised sensors when infection occurs, re-routing the new measurements to the other sensors in the network until the issue is resolved.

Maintainability can be described as the capacity to configure, reconfigure, and update a system or part of a system. This security requirement is crucial in the IIoT paradigm, as the software in IIoT devices must have the capacity to be updated to be protected against previously unknown cyberattacks [59]. Updating software is considered a valuable counter-measure against various threats, as it helps to continuously modify firewall configurations at the edge of the network once the IDS detects new threats. Additionally, software vulnerabilities can be restored by utilizing software patches in routine software updates.

 doi:10.20944/preprints202307.0771.v1

5.5. Privacy

Privacy is a significant security requirement for individuals, companies, and governments. Due to the emerging demand for cloud storage services, privacy preservation has become a critical issue [60]. Modern devices generate variable amounts of data, making users susceptible to privacy violations, in which detailed profiles can be created for users from the generated data without their permission [61]. Additionally, applications can violate privacy by revealing personal information about a user's habits, movements, and interactions with other users [62]; for instance, the location of a user could be tracked by one of the applications they install on their devices.

Moreover, some websites (e-commerce websites, in particular) collect information about users, such as previous visits to products, shopping carts, and even credit card information. The collected information might be released to other companies without the user's permission. Another challenge is data capturing in transit, which may reveal personal information about people and objects.

5.6. Security Monitoring

Dynamic security monitoring of systems behavior is provided by famous tools known as IDSs. These tools can detect threats targeting networks and provide the required response procedure. It is substantial for any network—including IIoT environments—to monitor communications, identify threats, and respond to known and unknown intrusions, if needed [63–65]. One reason underlying the importance of IDSs is that old and less-secure devices (i.e., those which are difficult to patch to deal with known vulnerabilities) could connect to the network, which demands continuous security monitoring [66]. These devices might become a target of a DDoS attack. Then, they may become part of a botnet that can launch attacks against other legitimate IIoT devices in the network.

Capturing and investigating exchanged data, networks, and services using passive network traffic monitoring and analysis systems are of paramount significance in coordinating networks and identifying security issues in a timely manner [67–69]. The IDS can be identified as a tool that monitors network traffic to detect attacks compromising the CIA model of a given information system [70].

An IDS can be operated in three phases. The first phase is responsible for monitoring traffic or data, which depends on host- or network-based sensors. The second phase is responsible for analyzing the captured network traffic or collected data. This phase utilizes feature extraction or pattern identification techniques to accomplish the task. The third phase involves detecting threats using two well-known approaches: Misuse detection and anomaly detection [71].

Misuse-based intrusion detection methods gather known signatures and patterns of familiar threats in a database and compare incoming traffic with the database entries to detect attacks [72]. Misuse-based intrusion detection techniques have disadvantages, such as the high cost of signature matching, increased number of false alerts, and overload of network datagrams [73]. Additionally, the memory constraints of IIoT devices make it difficult to implement misuse-based IDS in those devices, due to the burden of a large number of signature entries in a database [74]. Moreover, the databases assigned for attack signatures and patterns must be periodically updated. Misuse-based IDSs require previous knowledge to be able to identify suspicious activities. Thus, unknown attacks may not be detected by this type of IDS [75].

Anomaly-based IDS methods maintain the situation in which normal data are generated by genuine devices in the network, and assess monitored data accordingly to identify anomalies (i.e., outliers that deviate from the normal data) [76]. These outliers are usually generated from noise or other incidents, which could result from utilizing a hacking tool. Therefore, unusual activities resulting from the existence of attackers would leave footprints in the infected network [77]. Therefore, attacks (including unknown ones) can be detected by anomaly-based IDSs using these footprints. In short, an anomaly-based IDS method creates a pattern of normal data generated by legitimate devices in the network, updates the pattern periodically, monitors network traffic in real-time, and compares the monitored traffic with the normal pattern; if any deviation from the normal pattern exists, it may indicate an intruder [78].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 July 2023 doi:10.20944/preprints202307.0771.v1

5.7. Secure Data Sharing

Securing data is one of the most important features of every digital paradigm, including IIoT. Various research papers have described data confidentiality as a substantial security requirement [79–82]. However, integrity and availability have a quantifiable economic effect and, hence, are considered more important than data confidentiality in traditional industrial settings [83,84]. Due to the evolution of the ICS as an integral part of the IoT paradigm, data confidentiality significance has become intelligible, due to the interactions in the ICS between devices and users that generate private data.

Companies consider secure data sharing an important security requirement to integrate Industry 4.0 [85,86]. Additionally, some companies have hesitated to employ data sharing-based approaches, such as smart maintenance, fault detection and prevention, and cloud services, as they believe that the data exchanged from their facilities to service providers might not be sufficiently protected [87]. Other researchers have supported the sentiment that organizations are hesitant to deploy cloud services or depend on cloud providers to supply data storage and sharing to customers [88]. Another serious challenge occurs when data breaches occur internally.

The exist various other challenges related to IIoT devices, applications, and environments. Data security techniques must be light to be equipped in IIoT devices with limited resources. Additionally, these techniques should be able to operate on heterogeneous devices. Some critical IIoT applications demand a full-fledged data security mechanism and, so, it is infeasible to implement the mechanism on a resource-constrained device (i.e., an edge node is favorable). Moreover, data security is important as, in industrial settings, it is important to share data to enable various intelligent capabilities; therefore, the data are usually sensitive [89]. An important characteristic of Industry 4.0 is the utilization of available data in an intelligent and efficient manner. Thus, the ability to share data with other entities in an Industry 4.0 environment or outside the environment's boundaries is significant to fulfill this requirement.

6. IIoT Attack Categories

IIoT environments comprise various devices, ranging from tiny embedded systems to full-fledged servers. Thus, it is significant to highlight the security challenges at different IIoT layers. As shown in Figure 5, the traditional IIoT layer architecture consists of three layers: The perception layer, the network layer, and the application layer. Each layer has its own enabling technologies and unique features. Thus, in this section, we discuss these three layers and the challenges IIoT applications encounter when applying security requirements in industrial environments [90]. Table 3 depicts popular attacks that target the three IIoT layers, along with their common countermeasures.

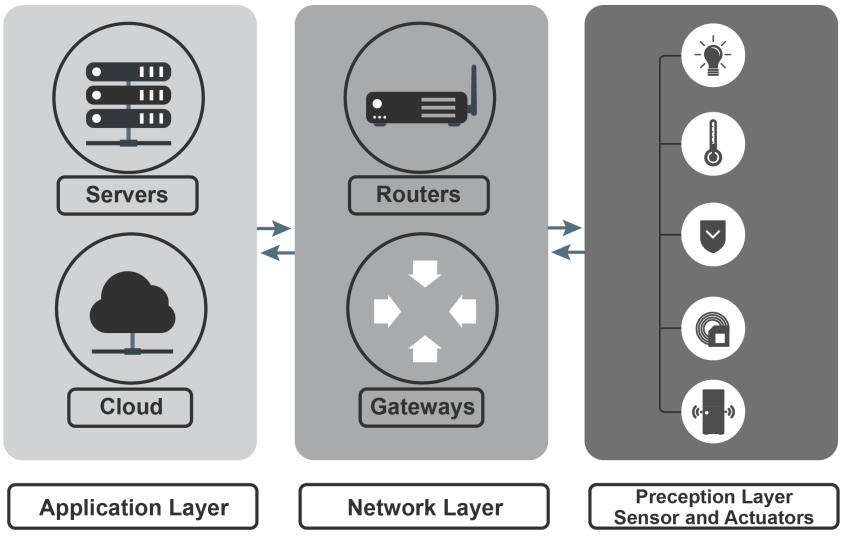

Figure 5. Framework of the three traditional IIoT layers: Perception, network, and application.

Table 3. Popular security threats that target the three IIoT layers and their common countermeasures.

Layer	Attack	Violated requirements	Common counter-measures
Perception	Node Capture	Confidentiality, Authentication	Abolishing information related to secure keys after disassociation [91]
	Jamming	Availability	Increasing interference resistance using techniques such as FHSS [92] and DSSS [93]
	Sleep Deprivation	Availability	Ensuring security policies are not violated using policy-based IDS [94]
	Replay	Integrity	Utilizing timestamps and nonces [95]
Network	Selective-Forwarding[a]	Availability	Detection and prevention using a combination of IDS and IPS [96]
	Eavesdropping	Confidentiality, Privacy	Employing access control and data encryption techniques [97]
	Sybil and ID Cloning[b]	Authentication	Applying packet filtering, IDS, and localization techniques [98]
	Wormhole	Confidentiality, Availability	Deploying secure neighboring discovery techniques and measuring challenge-response and RTT delay [99]
	Denial of Service	Availability	Utilizing traffic filtering, IDS, and tracking techniques [100]
	Man in the Middle	Confidentiality, Authentication	Employing light encryption techniques and deploying IDS [101]
	Sinkhole	Availability	Employing IDS and IPS to detect and prevent this threat [102,103]
	Blackhole[c]	Availability	Utilizing various routing paths and deploying IDS and IPS techniques [104]

Table 3. *Cont.*

Layer	Attack	Violated requirements	Common counter-measures
Application	Malicious Code Injection	Confidentiality, Authentication	Employing private-key cryptography, light public-key encryption, and authentication mechanisms [105]
	Cross-site or Malicious Scripts	Confidentiality, Authentication	Deploying signature-based IDS and content and pattern analysis techniques [106]
	Malware Injection	Integrity	Deploying IDS, IPS, and malware removal mechanisms [107]
	Data Distortion	Integrity and secure data sharing	Utilizing access control, encryption, and recovery [108] such as backup mechanisms
	SQL Injection	Confidentiality, integrity	Utilizing parameterized statements, IDS, access control, and encryption techniques [109]
	Ransomware	Confidentiality, Authentication	Employing traffic filtering, IDS, IPS, and encryption techniques [110]
	Side-channel	Confidentiality	Protection of cryptography techniques, preventing traffic analysis, and enforcing strict access control policies [111]
	Authorization and Authentication	Authentication and access control	Using access control and authentication techniques [112]

a also known as Grayhole. b a.k.a. malicious cloning. c sometimes referred to as selfishness

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 July 2023 doi:10.20944/preprints202307.0771.v1

6.1. Perception Layer Attacks

The perception layer (a.k.a. device layer) consists of devices equipped with various objects, such as sensors, cameras, robots, and smart meters. This layer is responsible for identifying and gathering information related to the target sensor. This information comprises measurements of quantities such as movement, chemicals in a specific environment, vibrations, heat, acceleration, or humidity. The collected data are transmitted to the lower layer (i.e., network layer), and eventually conveyed to an information processing system [113]. This subsection concentrates on attacks targeting the perception layer.

6.1.1. Node Capture Attacks

The attacker in this kind of attack can physically obtain or replace an IIoT node or modify certain hardware. This type of malicious act leads to exposing sensitive information related to digital rights coordination, such as cryptography keys or access keys. Once the attacker gains access to the IIoT device, they can then malignantly act to harm other devices in the network [114].

6.1.2. Jamming Attacks

This type of attack can disrupt or alert communication of IIoT devices by tampering or interfering with the access mode of wireless communication. Thus, IIoT devices will be prevented from transmitting data to other network entities successfully [115]. Attackers can jam the wireless signal remotely utilizing a powerful passive transmitter. They can also use shielding techniques to avoid defensive mechanisms. Radio noise that matches the frequency of a specific system can be utilized to interfere maliciously with RFID systems.

6.1.3. Sleep Deprivation Attacks

This family of attacks prevents IIoT devices from resetting to sleeping mode by inserting infinitely looping codes into the device's memory or making hardware modifications. By default, IIoT devices are battery-constrained and remain on sleep mode when they do not transmit or receive information, to preserve battery; however, these attacks can drain the batteries of IIoT devices by actively waking them up, eventually shutting them down completely (this is a type of DoS attack) [116].

6.1.4. Replay Attacks

Without authentication mechanisms, an intruder can capture a previously legitimate message transmitted from an IIoT device to another entity, then modify and replay the message to its final destination [117]. This kind of attack is possible when the authentication is applied in a certain IIoT environment. The intruder can eavesdrop on the wireless channel, capture the message, clone, and use the authentication code in the captured message (i.e., generated by the sender).

6.2. Network Layer Attacks

Once the data are handed from the perception layer to the network layer, the network layer identifies the path the message takes to reach the receiver (this path includes the first edge router, which is responsible for forwarding the message to the next router on the route) [118]. The aim of the network layer is to transfer network packets (a.k.a. datagrams) between heterogeneous networks transmitted by various IIoT devices. These network packets are sent by the IIoT device interface using a communication protocol, passing through various communication links [119].

6.2.1. Selective-Forwarding Attacks

A selective-forwarding attack is a type of DoS attack. In this attack, the attacker may choose to forward certain packets (e.g., RPL control messages) and drop the rest of the packets, to disrupt the

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 July 2023 doi:10.20944/preprints202307.0771.v1

route [120]. This attack can have more severe consequences when combined with other attacks, such as sinkhole attacks.

6.2.2. Eavesdropping Attacks

This type of attack enables the intruder to listen to the ongoing exchange of messages between IIoT devices in the communication channel. The message exchange can include sensitive information, including passwords and bank information in plaintext if encryption is not applied [121].

6.2.3. Sybil and ID Cloning Attacks

A Sybil attack occurs when an intruder steals the identity of a legitimate IIoT device to disturb the communication between devices. Additionally, an intruder can maliciously possess various identities to deceive IIoT devices into believing many IIoT devices are in the network [122]. On the other hand, a Clone ID attack can be defined as spoofing a legitimate node's identity and pretending that the attacker has the identity of another legitimate node in the network. This attack can be launched by an attacker to access more devices in the network [123].

6.2.4. Wormhole Attacks

This type of attack allows two attackers to create a virtual long-distance tunnel, which is created to force the other devices in the network to transmit their packets through that tunnel [124,125]. Additionally, the exchanged information could pass through the intermediate legitimate nodes, to drain their batteries [126].

6.2.5. Denial of Service (DoS) Attacks

An intruder can launch this type of attack to sabotage bandwidth or network resources, which can be accomplished by actively transmitting a large number of packets to the devices/servers connected to the network indefinitely or temporarily, to make them busy and eventually prevent them from doing their usual activities. This attack might also drain the batteries of IIoT devices, leading them to completely shut down [127,128]. Another subset of DoS attacks is DDoS, which compromises normal IIoT devices that do not have appropriate security protection to become a source of attack traffic. This attack can be categorized into two classes: Logical and flooding [129]. A logical attack allows the intruder to transmit deceiving messages to misguide normal users into believing that the application or service of the service on the machine that they are contacting is unavailable (i.e., fully occupied). A flooding attack targets edge IIoT devices or servers by transmitting numerous amount of packets, making the target devices unable to process these packets and eventually become unavailable to normal users in the network (i.e., they cannot reply to normal requests from legitimate users) [130,131].

Edge computing is more susceptible to DoS attacks than cloud computing, as services are provided by edge IIoT devices, which cannot be equipped with suitable defense mechanisms due to computational limitations. Additionally, attackers target edge devices and use them as sources to launch attacks on nearby edge servers; hence, the attacks may be more severe, compared to when targeting far-away cloud servers (in which case, the traffic would pass through various routers and might be blocked before it reaches the cloud server). In this regard, a memorable case is when 65,000 IoT devices were targeted and exploited to launch malicious packets against famous services such as Dyn[1], Kerbs[2], and OVH[3]; this attack is known as Mirai botnet [132].

---

[1] A company that offers services to control, coordinate, and optimize online infrastructure.
[2] A daily blog that covers cyberattacks.
[3] A giant European hosting provider.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 July 2023 doi:10.20944/preprints202307.0771.v1

6.2.6. Man in the Middle Attacks

The attacker can launch this attack to become a "man in the middle" of ongoing communication between two legitimate IIoT nodes. The attacker then can monitor the communication in real-time, as well as intercepting and altering the exchanged messages [133].

6.2.7. Sinkhole Attacks

The intruder launches this attack to lure network entities to believe that it is the sink node (i.e., a node in a network with stronger capabilities than other nodes in the network), to forward network traffic to it. The forwarded traffic is eventually transmitted to the attacker, and might not reach the intended receiver [134].

6.2.8. Blackhole Attacks

This attack can be launched by a malicious node that acts as a hole (a node that forces the other network entities to route the packets to it and drop the forwarded packets), to degrade IIoT network performance [135].

6.3. Application Layer Attacks

The last layer in the traditional IIoT layer architecture is the application layer. The application layer is responsible for presenting data and providing IIoT users with various applications, such as smart transportation, smart manufacturing, and intelligent logistics [136]. The application layer is susceptible to various security issues, listed as follows:

6.3.1. Malicious Code Injection Attacks

Attackers can exploit the vulnerabilities associated with the debug modules to inject malicious codes. Once the attackers inject the malicious codes, the attacker can then perform unwanted activities on the affected device [137]. Additionally, the attacker may be able to carry out malicious activities on the entire network through the affected device. Additionally, IIoT devices can be infected when they upgrade their firmware/software using an OTA utility. More specifically, the attacker can inject a virus into the IIoT device when the device is installing a scheduled firmware update; hence, this action demands rebooting the IIoT device to be effective. To protect IIoT devices from such attacks, there should be a suitable authentication mechanism and identification for the edge devices, as well as ensuring that the updates and upgrades that can be installed on IIoT devices are trustworthy (i.e., do not carry malware).

6.3.2. Cross-site or Malicious Scripts Attacks

These vulnerabilities can be exploited by malicious nodes, through websites visited by IIoT users. Particularly, suspicious websites could be equipped with malicious scripts that decoy the user's system to become infected, thus revealing the user's data [138]. Such malicious scripts can be created using any scripting language, such as JavaScript, like any other legitimate script, and run by any Internet browser. One possible threat of cross-site and malicious scripts is their ability to lure users to upload data, even without verification [15].

6.3.3. Malware Injection Attacks

In this type of attack, the intruder targets a victim edge device's service requests to inject malware into that device's system or the network [139]. This attack leads to disruptive threats to system security and data integrity. Both edge servers and devices are susceptible to this kind of attack. The edge server can be targeted by a malware injection attack known as SSI. This attack can be categorized into four classes: XML injection, CSRF injection, XSS injection, and SSRF injection. Edge devices are prone to a

 doi:10.20944/preprints202307.0771.v1

malware injection attack known as DSI (e.g., RCE or reaper), in which the attacker injects malicious code into the targeted IIoT device [140,141].

6.3.4. Data Distortion Attacks

In this type of attack, intruders eavesdrop on the wireless channel, intercept the packets transmitted between network entities, distort them, and forward them to the receiver [142].

6.3.5. SQL Injection Attacks

This type of attack exploits the vulnerabilities of applications that retrieve and transmit information from and to the databases. This family of attacks can also modify the running SQL query by maliciously launching a query fragment; for example, through a web form. Consequentially, the attacker can gain access to the database and alter the database schemes, tables, tuples, or attributes [143].

6.3.6. Ransomware Attacks

A ransomware attack is a subset of the malware attacks family, where the attacker hijacks IIoT devices or files and asks for compensation (usually money) to restore access to IIoT devices or decrypt files, such that the victim device can use them again. The cyber-criminals who launch this type of attack usually interact with the victims and ask them to pay a ransom (e.g., Bitcoin) in exchange for decrypting the files or regaining access to the IoT devices [144].

6.3.7. Side-channel Attacks

This type of attack utilizes publicly available data (i.e., insensitive data) to deduce confidential data by relating it with the user's private data. The attacker takes advantage of publicly available data on the edge computing infrastructure and feeds them as input to ML, DL, or anonymous algorithms to generate the desired output (e.g., sensitive information). Side-channel attacks may target any network entity, and intruders can utilize various methods to launch side-channel attacks, such as timing attacks, cache attacks, and electromagnetic attacks [145–147].

6.3.8. Authorization and Authentication Attacks

In these types of attacks, the intruder utilizes fake credentials to gain access to protected resources. Ordinarily, edge servers and devices are authenticated in edge computing, to authorize edge devices to gain access to the services or resources placed on the edge servers. These types of attacks can be classified into four groups: Threats that exploit authentication methods, threats that target authorization protocols, dictionary attacks, and over-privileged attacks [148].

In a dictionary attack, the attacker creates a file of the most-used passwords and tries every possible password in a matter of minutes, to determine the correct credentials that allow the attacker to gain access to the resources of a specific user [149]. In authentication and authorization protocol attacks, the adversary exploits authorization or authentication vulnerabilities to reveal the authenticated user's credentials, thus gaining access to the resources or services at the edge servers as an authorized user. In over-privilege attacks, the intruder can shut down or gain access to the system as an authorized user by inserting malware. This attack can be launched in various forms, such as changing a smart home door pin and retrieving and utilizing the user's voice records [150].

7. State-of-the-Art of IIoT Secure Deployment on Edge Computing

Various IIoT edge computing entities utilize communication protocols, sensing capabilities, and data processing techniques to interact with each other, accomplishing various advances in many applications. Edge computing plays an integral role in enhancing the performance of the IIoT paradigm. For example, low latency has become one of the main characteristics distinguishing edge computing

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 July 2023 doi:10.20944/preprints202307.0771.v1

from cloud computing, thus enhancing the performance of real-time applications. Additionally, edge computing improves the security of IIoT environments, to some extent. However, traditional security mechanisms cannot be directly applied to edge computing and completely satisfy the security requirements discussed in Section 5, as it is difficult to predict security risks when designing the security model. Furthermore, the security threats related to networks, data, or applications emerge as technologies are integrated with each other (i.e., adopting edge computing to IIoT environments will bring more threats to the IIoT paradigm related to edge computing). Some well-known security risks related to the integration of IIoT and edge computing, as well as state-of-the-art solutions aimed at these risks, are discussed in this section.

7.1. Network Layer Security

An attack launched from the edge network could threaten all of the edge functional entities, and may propagate to the whole communication network (e.g., eavesdropping on the communication link or injecting malicious traffic to the broadcast address in the network) [151]. Intrusion detection and prevention are two important research interests proposed to protect edge network security in IIoT environments. Many current solutions to combat IIoT network layer attacks rely on emerging technologies, such as AI- and Blockchain-based solutions, to provide the necessary detection and prevention mechanisms, as detailed in Table 4. For example, Diro and Chilamkurti [152] have utilized the LSTM algorithm to detect attacks on distributed fog environments that might target IIoT devices. This technique is the first step to improving the security of fog computing, by accurately and precisely detecting various attacks that might degrade the network performance and malfunctioning network entities. The authors validated the proposed technique using two data sets—ISCX[4] and AWID[5]—and compared the proposed method with LR. The technique yielded a promising accuracy of 98.22% on the AWID data set and 99.91% on the ISCX data set. The proposed technique was better than LR by 9% on the ISCX data set; however, it took a significantly longer time to train the proposed method, compared to LR.

[4] Found at https://www.unb.ca/cic/datasets/ids.html
[5] Found at https://icsdweb.aegean.gr/awid/

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 July 2023 doi:10.20944/preprints202307.0771.v1

Table 4. Summary of works focused on enhancing the security of the IIoT network layer.

Scope	Ref.	Algorithm	Resolved issue	Data set	Performance metrics
Deep learning-based IDSs	[152]	LSTM	DoS attacks	ISCX, AWID	98.22% accuracy on AWID, 99.91% on ISCX
	[153]	Stochastic MC	false injection	Custom	NA
	[154]	LSTM and 1D CNN	DDoS	DoS2019	1D-CNN: 99.3% precision, 98.9% recall, 99.1% F1-score[a]
	[155]	ANN, RNN-LSTM, RNN-GRU	botnet attacks	BotIoT	ANN: 99% accuracy, RNN[b]: 98% accuracy
	[156]	Stacked deep autoencoders	botnet attacks	N-BaIoT	3% improvement
	[157]	LAE and B-LSTM	botnet attacks	BotIoT	93.17% (binary), 97.29% (multiclass)
	[158]	RNN	botnet attacks	BotIoT	99.75% recall, 99.62% precision and F1-score
	[159]	CFBPNN	botnet attacks	5 datasets	100% accuracy
	[160]	Custom algorithm	botnet attacks	N-BaIoT	99.76% accuracy, 99.68% F1-score, 0.2250μ^c testing time
	[161]	Federated DL	zero-day botnet	Bot-IoT, N-BaIoT	Bot-IoT: 99.79% accuracy, 99.51% precision, 96.27% recall, 97.68% F1-score. N-BaIoT: 99.00% accuracy, 96.87% precision, 97.24% recall, 96.88% F1-score
	[162]	Federated DL	DDoS attacks	UNSW NB-15	98% accuracy
Signature-bawed IDSs	[163]	Custom algorithm	routing attacks	NS2[d]	95.0% detection rate, 1.23% FPR[e]
	[164]	Custom algorithm	SQL injection	Custom	4.7× improvement
	[165]	Custom algorithm	DDoS attacks	Custom	Not reported
	[131]	Custom algorithm	DDoS attacks	Custom	Up to 99.84% detection rate, as low as 129ms testing time
	[166]	Fuzzy logic	Blackhole attacks	Custom	more than 90% accuracy
	[167]	Node ranking	sinkhole attacks	NS3	96.19% detection rate, 4.16% FPR, 4.04% FNR[f]
	[168]	Parallel ABC	Sybil attacks	Simulation	Approximately 97% accuracy, 97% sensitivity
	[169]	XGBoost	botnet attacks	BoT-IoT	99.99% accuracy, 97.5% recall, 99.5% precision, 98.5% F1-score
	[170]	Gaussian distribution and local search	Mirai and Gafgyt botnets	N-BaIoT	90% in multiclass classification
	[171]	Dynamic analysis	botnet attacks	Custom	98.1% to 91.99% accuracy
	[172]	Fisher-score and XGBoost	botnet attacks	N-BaIoT	99.96% average accuracy

a The results of the LSTM-based approach were less accurate; so, the better-performing method is reported in this cell. b Both RNN-LSTM and RNN-GRU have identical accuracies. c This symbol represents time in microseconds format. d NS stands for network simulator. e False positive rate. f False negative rate.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 July 2023 doi:10.20944/preprints202307.0771.v1

Chekired *et al.* [153] have proposed a distributed and hierarchical intrusion detection system to detect attacks targeting the fog architecture. The proposed solution was mainly designed to detect false data injection attacks that target smart meters in the power grid. The proposed technique consists of three layers: AMI, fog, and cloud. Each layer incorporates various IDSs that hierarchically detect intrusions in a cooperative manner. The fog layer assimilates three types of IDS: Fog IDS, residual area network IDS, and HAN IDS. The authors then adopted a stochastic MC to differentiate malicious activities from normal traffic. The authors demonstrated the effectiveness of the proposed technique using real electricity data generated from Toronto.

Huang *et al.* [154] have presented a defense approach to prevent DDoS attacks in IIoT environments. The proposed technique relies on a multi-point collaborative capability, deployed at the edge to detect DDoS attacks and protect IIoT devices from adversaries. The collaborative defense aspect of the proposed technique is accomplished through the use of blockchain technology, which is adopted to securely distribute defense information throughout the IIoT environment. Additionally, the authors introduced a swift defense information distribution technique, to minimize the information sharing latency and enable the proposed method to respond promptly. The authors also employed two deep learning-based mechanisms to differentiate normal traffic from attacks using an LSTM-Attention network, the attack traffic was further categorized, and the attacks were detected using a 1D CNN architecture. Furthermore, the authors used the classified attack feature representations to acquire new feature information and, hence, produce defense information and improve the robustness of the security system. The classification part based on deep learning was evaluated and compared with baseline models (i.e., SVM, MLP, and *k*NN). The deep learning-based techniques obtained superior results, compared to the baseline models, in terms of precision, recall, F1-score, and accuracy. Experiments conducted on the DoS2019 data set[6] also demonstrated that the swift sharing approach could decrease the propagation delay when distributing the information, thus enhancing the response time and better protecting the devices from DDoS attacks. The proposed LSTM-based approach achieved high performance in three performance metrics (i.e., 99% precision, 98.7% recall, and 98.8% F1-score), while the 1D CNN-based method achieved slightly better results than the LSTM-based approach (i.e., 99.3% precision, 98.9% recall, and 99.1% F1-score).

Mudassir *et al.* [155] have presented three accurate deep learning-based approaches capable of detecting botnet attacks that target the IIoT environment. The three techniques are based on ANN, RNN-LSTM, and RNN-GRU, respectively, and were evaluated on the BotIoT data set. The ANN-based approach achieved the highest performance, in terms of accuracy (99%), although the other techniques obtained similar accuracies (98%). However, the RNN-GRU-based techniques performed slightly better in terms of detecting attacks with minimum samples, such as DoS and DDoS targeting HTTP protocol. The performances of the three models, in terms of precision and recall, were not high, particularly in classifying attacks with a small number of samples. Thus, the authors improved their performance by under-sampling the majority class to create a balanced data set. The proposed methods achieved better results, in terms of precision and recall, on the balanced data set. However, deploying such techniques on IIoT networks may pose an issue, considering the constraints of the devices, as the deployment of deep learning-based approaches typically requires high computation and memory usage.

Tsogbaatar *et al.* [156] have introduced a framework using an ensemble of deep learning models as a building block to detect IoT threats utilizing SDN. The proposed framework consists of three modules: An anomaly detector module, device status prediction, and smart flow management. Stacked deep auto-encoders are used to extract features and feed them into the ensemble deep learning model. The proposed system was evaluated on the N-BaIoT and costumed data sets, and accomplished superior results on even a 1% imbalanced data set, compared to related works, achieving an improvement of approximately 3% over a single deep learning model.

---

[6] Found at https://www.unb.ca/cic/datasets/ddos-2019.html

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 July 2023 doi:10.20944/preprints202307.0771.v1

Popoola *et al.* [157] have proposed using dimensionality reduction and intrusion detection techniques to identify threats in IoT environments. The dimensionality reduction part of the framework was based on LAE, while the intrusion detection part was based on B-LSTM. The authors analyzed the long-term inter-related changes using B-LSTM after the LAE had reduced the feature set to accurately identify network traffic samples. The proposed framework was validated on the BoTIoT data set, yielding promising results. The conducted experiments demonstrated that the utilized feature reduction technique remarkably improved the memory space, by approximately 92%, and performed better than state-of-the-art dimensionality techniques by up to 27%. The performance of the proposed framework, in terms of MCC, was high; obtaining 93.17% in binary classification scenarios and 97.29% in multi-class classification scenarios.

Popoola *et al.* [158] have introduced a botnet detection technique based on deep learning which is capable of dealing with imbalanced network traffic data. The authors adopted the SMOTE algorithm, which produces additional samples for classes with a small number of samples, to attain class balance. Consequentially, the authors fed the balanced data into a deep RNN to acquire knowledge of the hierarchical feature representations and, thus, distinguished attacks from normal traffic. The authors conducted two types of experiments using the BotIoT data set: Without and with the SMOTE algorithm. The first experiment proved that the imbalanced data affected the results (in terms of recall, precision, F1-score, AUC, GM, and MCC). On the contrary, the SMOTE-RNN-based approach yielded superior detection results, compared to state-of-the-art models, achieving 99.75% recall, 99.50% precision, 99.62% F1-score, 99.87% AUC, 99.74% GM, and 99.62% MCC. The proposed solution utilized the characteristic of RNNs, in terms of distinguishing samples in time-series historical data, which have achieved high accuracy in many fields, including intrusion detection systems. However, the time required to detect intrusions is not negligible, which is a key issue, as this technique must be deployed on resource-constrained edge devices.

Jayalaxmi *et al.* [159] have proposed a botnet detection technique based on deep learning to protect IIoT networks. This method adopts a CFBPNN architecture and a feature selection method known as CFS, in order to minimize the time required for the intrusions and improve the detection rate performance. Additionally, the authors utilized a time-series technique known as NARX to examine the elements that have a high impact on the target class, to anticipate the behavioral pattern. The authors conducted various experiments on five data sets to evaluate their proposed framework; namely, NF-UNSW-NB15, NF-CSE-CIC-IDS2018, NF-ToN-IoT, NF-BoT-IoT[7], and ToN-IoT-Windows[8]. The authors compared the proposed framework with various neural network models; the results indicated the perfect accuracy, outstanding F1-score, and good precision of the proposed model.

Alani *et al.* [160] have proposed an effective botnet detection method using packet inspection and machine learning. The proposed framework also utilizes a feature selection technique to reduce the feature set and the detection time. The feature selection method chooses only seven important features, extracted from the network packet fields. These features are fed into the machine learning algorithm, in order to train it. The proposed detection technique and feature selection capability achieved higher than 99% accuracy.

Popoola *et al.* [161] have introduced an FDL-based technique to detect zero-day botnet attacks and protect IoT edge devices from data privacy leakage. The authors presented an optimal DNN architecture to classify the captured network traffic. The models of the DNN architecture are independently trained in multiple IoT edge devices, remotely managed by a model parameter server, and local model updates are aggregated using the federated averaging algorithm. Various messages exchanged between IoT edge devices and model parameter servers were used to generate the global DNN model. The authors utilized two data sets to validate their proposed framework: BotIoT[9]

---

[7] These four data sets can be found at https://staff.itee.uq.edu.au/marius/NIDS_datasets/
[8] This data set can be found at https://research.unsw.edu.au/projects/toniot-datasets
[9] Found at https://research.unsw.edu.au/projects/bot-iot-dataset or https://ieee-dataport.org/documents/bot-iot-dataset

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 July 2023 doi:10.20944/preprints202307.0771.v1

and N-BaIoT[10]. The proposed framework presented a high performance in classification metrics and can ensure data confidentiality and privacy. As the training data are distributed between edge IoT devices, the required memory space and storage are minimal for each IoT device. Additionally, the framework is deployed over edge IoT devices, ensuring low latency. Li *et al.* [162] have deployed a similar approach, combining both FDL and edge/fog computing to protect IIoT environments from DDoS attacks. This method also achieved high detection accuracy (i.e., 98%).

Wazid *et al.* [163] have proposed an effective method to detect routing attacks launched by malicious neighbors, in order to target edge-based IoT environments and degrade the performance (particularly, the delay and throughput) of edge networks. This method was designed to detect routing attacks and can be deployed on edge servers to identify the suspicious nodes that launch the attacks on their neighbors. This method should be distributed on powerful servers, as the collected data would be huge, including routing messages that are sent to all the nodes in the network (i.e., broadcast messages).

Singh *et al.* [164] have introduced a network traffic monitoring system that thoroughly inspects incoming and outgoing network packets. The proposed system specifies signature rules to detect SQL injection attacks and other traffic injection attacks, places these rules in the IDS database, compares the packets with these rules and, if any deviation is found, the attack is detected. This method only detects one family of attacks: Traffic injection attacks. This kind of method belongs to misuse intrusion detection systems. The biggest issue with intrusion detection systems in this category is their lack of ability to detect novel attacks (i.e., attacks with no signatures in the database). The only solution is to update the signature rules placed in the database through historical attack data analysis, which takes time and effort.

Yan *et al.* [165] have presented a multi-layer framework to mitigate DDoS attacks. The framework collects network traffic at the cloud computing layer, classifies the traffic, and detects DDoS attacks based on the captured traffic. The authors utilized a data analysis mechanism located at the cloud computing layer to inspect the DDoS attack behavior. Consequentially, the inspection information is forwarded to the fog computing layer to mutually combat DDoS attacks.

Zhou *et al.* [131] have proposed a fog-based technique to mitigate DDoS in IIoT environments. The proposed system captures network traffic and analyzes it offline using VNFs in a local server. The analyzed network traffic information is matched with information captured at the cloud servers, to effectively detect and defend against DDoS attacks. The proposed method was designed to improve the response time and enable IIoT resource-constrained devices to efficiently adopt this technique without noticeable computational overhead. This approach consists of three levels and was implemented utilizing the Mero control system to achieve acceptable results. These methods were also designed to only detect one family of attacks (i.e., DDoS attacks), so they do not constitute a complete protection solution for IIoT environments.

Bhardwaj *et al.* [130] have proposed a proactive technique to mitigate DDoS attacks. The proposed method uses three components to effectively detect DDoS attacks: Locally deduced information, edge function, and web service. This approach is distinctive, as the detection is accomplished in real-time and provides defense responses. The authors claimed that the proposed solution could detect IoT DDoS attacks faster than related approaches by 10 times. Additionally, the authors claimed that the proposed approach could reduce the damaging impact of DDoS by 82%.

Simpson *et al.* [166] have proposed an approach based on fuzzy logic to detect cooperative attacks (i.e., a type of blackhole attack) targeting edge nodes in IoT environments. The authors presented a trustworthy infrastructure placed on the edge, to mitigate security risks in smart cities. This infrastructure was designed to detect malicious threats (cooperative attacks, in particular) in real-time. The authors position the detection mechanism on the edge computing platform to reduce

[10] Found at https://www.kaggle.com/datasets/mkashifn/nbaiot-dataset

 doi:10.20944/preprints202307.0771.v1

the computational overhead on IoT devices. Compared to services provided by the cloud, placing the detection method at the network's edge can decrease bandwidth utilization and delay. Once an attacker is detected, the node that launches the attack is isolated. The authors also proposed utilizing a reaction-based trust evaluation, which generates a reputation value to re-analyze suspicious entities. The proposed framework was evaluated, demonstrating its effectiveness in detecting cooperative attacks.

Zaminkar *et al.* [167] have presented a defense technique based on node rating and ranking to deter sinkhole attacks from affecting IoT devices. The authors conducted real experiments in industrial premises containing IoT devices and launched real-world sinkhole attacks using relevant tools. The authors captured real data frames flowing from and to IoT devices communicating with the APs through Wi-Fi (i.e., traffic transferred through wireless communication). Other network traffic transferring from the APs to a central switch and then to a router was captured as well (i.e., traffic transferred using wired communication). Network traffic was captured by switch port mirroring and the Wireshark sniffing tool. The authors deployed nine commercial IoT tools in the industrial environment, which acted as infecting devices, and formed two botnets to launch the sinkhole attacks.

Khan *et al.* [168] have introduced a smart communication mechanism that detects and prevents Sybil devices from targeting IIoT devices in PEC. Once the device masquerades as one of the IIoT devices (i.e., spoofs its identity), the adversary's identity is detected, and a notification is sent to edge servers to deter upstream messages transmitted from that suspicious node. The building block of the proposed framework is the parallel ABC algorithm, which determines the optimal network configuration for IIoT devices on each edge server once the attack is detected. Then, the server carries out job migration with the servers nearby, in order to improve the network performance and for load balancing, based on the capabilities of the nearby servers (e.g., storage and processing capabilities). The authors conducted an experiment to validate their detection and prevention techniques, proving that the technique is capable of detecting Sybil attacks and the delay can be reduced, the throughput could be improved, and the data communication of IIoT devices in PEC could be controlled with the help of the parallel ABC algorithm.

Lawal *et al.* [169] have proposed a fast and accurate anomaly- and misuse-based method to mitigate anomalies in IoT environments using fog computing. To ensure that an intruder is detected rapidly, the authors placed a list of IP addresses belonging to suspicious devices in a database (the signature-based part of the proposed system). Meanwhile, the anomaly detection part of the proposed framework adopted a machine learning technique known as extreme gradient boosting to differentiate malicious packets from genuine ones. The signature-based part was shown to be effective, in terms of detection time, when tested it on a data set (i.e., its detection time was faster than the anomaly detection part by more than six times). The anomaly-based part of the framework also demonstrated its effectiveness, achieving a 99% average accuracy and a 97% average recall.

Alharbi *et al.* [170] have introduced a neural network architecture, called local–global best bat, to detect botnet attacks in the IIoT paradigm. The proposed method efficiently chooses feature representations and hyper-parameters extracted from nine off-the-shelf IoT devices affected by attacks launched from two botnets: Mirai and Gafgyt. The bat's velocity in the swarm is reformed using the local–global best-based inertia weight. Additionally, the authors utilized a Gaussian distribution in the population initialization step, in order to overcome the bat algorithm swarm diversity problem. The Gaussian density function in each generation is followed by a local search, thus accomplishing ideal exploration. The authors used a publicly available data set (i.e., N-BaIoT) to validate their approach. This data set consists of eleven classes: ten classes representing botnet attacks and a benign class. The proposed model was shown to be superior, compared to existing weight-optimization techniques such as PSO, achieving an accuracy of 90% in multi-class classification.

Nguyen *et al.* [171] have adopted a dynamic analysis technique to enhance graph-based features and, hence, improve the IoT botnet attack detection performance. Printable string information is gathered using dynamic analysis when carrying out the instances. Consequentially, to traverse the

graph, the printable string information is effectively employed, based on static analysis, to obtain graph-based features and eventually differentiate benign instances from attack instances. The proposed method was evaluated using a data set of 8,330 samples, including 5,531 attack samples and 2,799 normal samples. The method yielded a promising accuracy of up to 98.1%.

Alqahtani *et al.*[172] have presented a feature selection method based on the Fisher score[11] and an IoT botnet attack detection technique based on XGBoost. The Fisher score-based feature selection method was utilized to choose the most important feature out of 115 available features, and the XGBoost-based method was used to distinguish between IoT botnet attacks and normal traffic. The authors conducted various experiments on the N-BaIoT data set and evaluated their approach, using 10-fold cross-validation and holdout methods. The proposed feature selection method reduced the feature set to three important features out of 115 available features, thus reducing the detection time, while the selected features along with the proposed detection technique improved the detection accuracy when compared to the case where the baseline features were used.

Arshad *et al.* [173] have introduced a lightweight IDS designed for the IoT paradigm, which best fits the requirements of constrained IoT devices. The proposed method can be implemented on IoT devices and edge routers collaboratively to improve detection accuracy, decrease false positive rates, and enhance visibility. The authors created attack signatures and placed them in a database; this database is then installed on IoT devices. Thus, each IoT device is equipped with a signature-based IDS. Furthermore, the edge-router learns the normal activities of the IoT devices, in order to detect any activity that deviates from the normal traffic. Thus, an anomaly-based IDS is positioned at the edge router. The effectiveness of the proposed solution was demonstrated, in terms of energy and memory consumption.

Arshad *et al.* [174] have designed a similar framework for energy-constrained IoT devices, which can detect intrusions in IoT environments. The proposed framework can be implemented on IoT devices utilizing the Contiki operating system and on edge devices, in order to protect IoT environments against increasing threats (particularly, botnet attacks), while considering their low energy consumption, less computational overhead, and minimum communication cost. As with the previous approach, the proposed method installs a signature-based IDS in the IoT devices while placing the anomaly detection IDS at the edge router. Each IoT device has three mechanisms: Network monitoring, system monitoring, and detection engine. The anomaly detector consists of two GDEs and three capabilities: Detection, correlation, and alert capability. The framework's efficacy was demonstrated, in terms of minimizing energy consumption and memory utilization.

However, the two previous approaches suffer from the following shortcomings: signature-based IDS could pose an issue for resource-constrained devices, due to the increasing number of attacks that need to be placed in the database and managed by those constrained devices. Additionally, new attacks should be added to the database; however, updating the database on each IoT device is cumbersome and consumes energy and memory resources. Moreover, the edge router is traditionally designed to forward network layer datagrams (i.e., it processes the network layer header); however, to deploy an IDS on the edge router, it is necessary to de-capsulate the packet to see the payload information, which violates end-to-end communication (i.e., the data should be transferred from the transport layer of the sender to the transport layer at the receiver).

Zhang *et al.* [175] have presented a method to prevent signature forgery attacks in IIoT environments using a robust certificate-less signature mechanism. The security of the proposed method was verified, and its effectiveness against malicious third parties and public key replacement threats was demonstrated.

---

[11] A representative filter-based technique employed to select important features and ignore insignificant features through minimization of intra-class distances and maximization of inter-class distances.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 July 2023 doi:10.20944/preprints202307.0771.v1

Qi *et al.* [176] have proposed a prevention scheme utilizing secure access control to ensure the security of data transmission (i.e., to prevent malicious data transmission issues) in the IIoT paradigm. The introduced technique relies on a ciphertext policy attribute-based encryption mechanism, which enables IIoT entities to apply fine-grained policies to coordinate access to IIoT data. The computational overhead of implementing the proposed technique on IIoT devices is reduced through the use of a hybrid cloud infrastructure, which handles the encryption and decryption processes. This method can also provide a new privacy capability to IoT data, known as item-level data protection; a capability that can deter key leakage issues.

Tajalli *et al.* [177] have adopted an average consensus-based mechanism to provide smart micro-grids (i.e., an IIoT application area) with optimal scheduling for real-time operations and to resist DoS attacks. The proposed method utilizes a fog layer to decrease delays and supply the necessary data storage and internal computation capabilities for the IIoT environment. The security of the proposed method was also tested in heterogeneous IIoT devices against various attacks (DoS attacks, in particular), in order to evaluate the method's performance in the context of such attacks. Their simulation results indicated the framework's effectiveness, in terms of accuracy, rapid response time, and feasibility.

7.2. Perception Layer Security

Edge nodes are resource-constrained: they are equipped with memories with limited storage capacity and micro/processors with limited data processing capabilities. Usually, these devices temporally sustain data transmitted by IIoT devices. Therefore, the complexity of data management is decreased; however, data security challenges (e.g., data leakage) may occur. Secure data storage is one of the hot topics relating to IIoT device deployment in the edge computing research area. As shown in Table 5, some solutions have been proposed recently to overcome such challenges.

Table 5. Summary of the works focused on enhancing data sharing and storage security.

Ref.	Method characteristics	Advantages	Limitations
[178]	Hybrid AES-RSA	It efficiently protects the secrecy of the data and enables devices to recover the data in a secure manner	It relies on RSA (i.e., an asymmetric encryption method), which is slow
[179]	Hierarchical and distributed	Large-scale and secure method capable of providing IIoT devices with status information of data storage	It is not linked to data and infrastructure characteristics
[180]	Combining super-increasing sequence and modified oblivious transfer	It efficiently provides secure data sharing and anonymity	It is centralized
[181]	Encryption outsourcing and fine-grained access control	It achieves encouraging response latency reduction and overhead saving for edge devices	The security analysis was not discussed in detail
[182]	Encryption with multi-authority cipher-text	Data access authorization and secure data sharing are ensured to protect edge devices against collusion attacks with low delay	The high scalability of edge networks might cause other security issues to emerge

Liu *et al.* [178] have introduced a framework to preserve data storage security utilizing a privacy algorithm known as local differential and a combined AES-RSA encryption technique. The authors adopted the encryption technique to jointly and efficiently protect the secrecy of the data while making it possible to recover the data in a secure manner (i.e., an entity with the appropriate key can recover the data). This framework consists of three layers: Local, cloud, and fog. However, the proposed approach utilizes the RSA encryption technique, which belongs to public key cryptography and is known to be slow.

Hi *et al.* [179] have utilized SDN technology to capture the data storage status information and, hence, facilitate secure data storage on fog computing nodes. In more detail, this approach designs trusted domains, security policies, and collaborative working schemes in a hierarchical fashion. The ultimate aim of this large-scale secure storage mechanism is to coordinate and authorize storage

 doi:10.20944/preprints202307.0771.v1

requests and provide data storage status information in a distributed manner, enabling IIoT devices to store and share data securely on the edge.

Ming *et al.* [180] have presented an efficient technique providing data privacy protection and secure data sharing, which can be deployed to protect devices that use fog computing services and resources. The proposed approach adopts an enhanced inadvertent transfer algorithm and utilizes edge low-latency services to enable vehicles to query the optimal driving route while providing these vehicles with location privacy protection and anonymity.

Xue *et al.* [181] have introduced a secure data sharing approach for VCC utilizing both cloud and fog computing paradigms. The proposed method was based on encryption outsourcing and fine-grained access control. The proposed framework provides the vehicles with privacy preservation and confidentiality in an efficient way; the computation overhead is securely separated from resource-constrained devices to cloud and fog servers. Additionally, response delay can be reduced while preserving the consumption of fog server resources with the help of vehicle mobility prediction and pre-pushing data to certain fog servers. The proposed method yielded a promising reduced response latency and overhead saving in edge devices.

Fan *et al.* [182] have introduced a data-sharing technique designed for vehicular fog computing, in order to securely recover stored data. The proposed method utilizes a novel encryption method with a multi-authority ciphertext mechanism, ensuring data access control in vehicular networks. The proposed framework also integrates an effective mechanism for attribute revocation. Therefore, vehicular network systems can effectively perform attribute revocation and execute data access authorization using the proposed framework, guaranteeing data sharing with low latency.

Adil *et al.* [183] have introduced an approach to identify jamming attacks utilizing edge nodes. The authors deployed three edge nodes equipped with different transmission frequencies in a WSN and used the RTT measurement of the transmitted signal to detect jamming attacks targeting the transmission channel. Even if one transmission channel (i.e., the one that an edge node is communicating through) is jammed, the other two edge nodes would be able to verify the wireless transmission serviceability in the WSN. Moreover, the RTT of the transmitted signal from the neighboring channel is also intermittent, compared to its usual time interval, due to interference in the neighboring channels. This interference indicates the existence of a jamming attack in the WSN. The proposed method was implemented using OMNeT++ and accomplished a detection rate of 94%.

Bany *et al.* [184] have proposed a protocol that deals with proactive jamming attacks targeting IoT networks. This protocol relies on the channel and routing assignment, and does not require new hardware or entities installed in the network or servers. The aim of this protocol is to enhance the overall packet delivery ratio of the IoT network in the context of normal activities performed by IoT devices, multi-channel fading, and jamming attacks. The introduced method comprises three steps: Path discovery, channel assignment, and route selection. The proposed method enhanced the packet delivery ratio in IoT networks, compared to existing protocols.

Abhishek *et al.* [185] have proposed a technique to detect jamming attacks in IoV networks. The authors mentioned that vehicular networks are vulnerable to jamming attacks, due to the nature of the shared wireless media through which the packets are transmitted. The authors focused on a type of Jamming attack in which the attacker waits until packets are transmitted, then the attacker jams the channel. This type of attack is severe, as the packet drop rate increases and the delay of the network is noticeable. Thus, sensitive applications that demand real-time communication would be disrupted. To solve this issue, the authors introduced a detection technique based on SVM to identify jamming attacks. To train the proposed method, the authors created a data set of packet drop probabilities obtained from jointly sufficient statistics. The proposed method was tested, and its effectiveness, in terms of detection ratio, was proven.

To summarize this section, we can make some observations related to the state-of-the-art methods. Devices, networks, and exchanged data between devices could all be targeted by cyber-criminals in various communication systems. However, the difference when securing the deployment of IIoT

 doi:10.20944/preprints202307.0771.v1

devices in edge or fog computing is that the significance of edge security expands when the data are downgraded to edge devices. The traditional protection of the exchanged data between IIoT edge devices, edge computing-based IIoT networks, and the devices themselves is low, while the complexity of the network that involves both heterogeneous IIoT devices and edge servers is high. Thus, proposing and standardizing new approaches that protect edge networks or data sharing is difficult, particularly when considering methods that require changes in the hardware, standardized communications protocols, or existing infrastructures.

For those approaches that do not impose changes to the hardware, communication protocols, or existing edge network infrastructure—for example, IDS approaches that detect various edge computing IIoT attacks such as injection attacks, DDoS attacks, and routing attacks—it is necessary to provide a solution that is lightweight and accurate. In this line, the proposed solutions for secure data sharing need to be further improved and investigated. These solutions are still limited and may become a hot topic in the near future. The use of emerging technologies, such as Blockchain and AI, could add value to the secure data sharing and management research area.

7.3. Application Layer Security

This subsection discusses the work proposed to secure the IIoT application layer. Table 6 compares those works focused on improving application layer security.

Dovom *et al.* [186] have introduced a framework that detects and categorizes malware, especially in IoT and IIoT environments, by diverting the program's OpCodes into a vector space and adopting both fuzzy and fast fuzzy pattern tree mechanisms. The fast fuzzy pattern tree-based technique achieved acceptable accuracy and good detection time. The framework also utilizes both robust feature extraction capability and a fuzzy categorization component. These components enable the framework to become a typical edge computing method that detects and categorizes malware. The only issue with this system is its reliance on fuzzy logic, which is known to be inaccurate when predicting unseen samples.

Table 6. Summary of works focused on enhancing the security of the IIoT application layer.

Ref.	Algorithm	Resolved issue	Data set	Performance metrics
[186]	Fuzzy pattern tree	malware	Kaggle[a] and Vx-Heaven[b]	97.0427% and 88.76% accuracies
[187]	LSTM	malware	UNSW-NB15	70% accuracy
[188]	Fuzzy set theory and a new loss function	malware	Drebin [189] and AndroZoo[190]	9% F1-score improvement
[191]	Fuzzy clustering	malware	Custom data sets created from VirusShare[c], Kaggle, and RansomwareTracker[d]	VirusShare: 94.66%, Kaggle: 97.56%, RansomwareTracker: 94.26% accuracies
[192]	Theoretical analysis	malware	NA	NA
[193]	J48	ransomware	VirusTotal	97.1% detection rate
[194]	*k*NN with DTW capability	ransomware	VirusTotal	Window size 15: 94.27% accuracy, 95.65% recall, 89.19% precision, 92.31% F1-score
[195]	Decision tree and naïve Bayes	ransomware	Custom	Packet-based (decision tree): 97.92% accuracy, 97.90 precision, recall, F1-score flow-based (naïve Bayes): 97.08% accuracy, 97.72% precision, 97.71% recall and F1-score
[196]	Random forest	ransomware	ransomware and malware-trusted	97.817% average F1-score of five splits
[197]	Logistic regression	ransomware	created from VirusShare website	96.3% detection rate and 99.5% ROC curve
[198]	DNN	ransomware	generated from VirusTotal	93% accuracy

a Found at https://www.kaggle.com/c/malware-classification. b Found at https://archive.ics.uci.edu/ml/datasets/Malware+static+and+dynamic+features+VxHeaven+and+Virus+Total. c Found at https://www.virusshare.com/. d Found at https://ransomwaretracker.abuse.ch/.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 July 2023 doi:10.20944/preprints202307.0771.v1

Guizani and Ghafoor [187] have presented a software-based framework that adopts NFV technology to resist malware diffusion in heterogeneous IoT environments. To deploy a precise countermeasure, the authors deployed a deep learning-based IDS to detect a broad range of malware promptly. The designed IDS is based on a combination of two well-known deep learning algorithms (i.e., RNN and LSTM). Once the malware is detected, the framework provides software or operating system update to address the security vulnerability that enables the attacker to break into the system.

Khoda *et al.* [188] have observed the fact that several IDS data sets lack a balance between the classes in the training set (i.e., the number of samples for the benign class is much higher than the number of samples for the attack class), which may affect the performance of machine learning-based IDSs. Thus, the authors presented an over-sampling[12] technique to deal with this problem. The framework also introduces two capabilities to detect edge computing malware in a unique way. The first capability utilizes fuzzy set theory, while the second one uses a new loss function capable of dynamically prioritizing malware samples. The proposed framework accomplished superb results, compared to related techniques. The method achieved an improvement in terms of the F1 performance metric, which reached over 9% when compared to related work.

Alaeiyan *et al.* [191] have introduced an edge layer deployable multi-label malware detection system-based fuzzy clustering. This system enables CPS networks to accurately predict malware threats. The Opcode frequencies are represented as a feature space, which is used with the proposed framework to conduct statistical analysis and differentiate malware categories. The proposed method was evaluated using three data sets, in which a high performance was achieved, in terms of accuracy.

Ogundokun *et al.* [199] have proposed a detection technique based on machine learning to identify ransomware attacks targeting IoT devices. Experiments were conducted using a laptop computer, a projector, and an Android device. Along with detecting ransomware attacks, the proposed system monitors the power consumption of IoT devices operating processes every 500 *ms*, using Power-to-track. The proposed method achieved acceptable performance in four metrics: Accuracy, recall, precision, and F-score.

Shen *et al.* [192] have investigated IoT malware spread behavior to determine the best possible malware detection techniques for protecting the privacy of IoT smart objects and preventing the spread of malware. The authors introduced a joint cloud-fog infrastructure and deployed an IDS to detect malware capable of overcoming the heterogeneity of smart sub-nets and the limited resources of IoT devices. Due to the smart object malware uncertainty, the authors also applied a signaling game to reveal the communication between the IoT devices and the corresponding edge nodes. The authors also detailed some related mechanisms, such as theoretically calculating the optimal Bayesian equilibrium of the game to enhance malware identification probability. Additionally, the researchers explored the factors influencing the optimal probability of an IoT device spreading malware, as well as factors that affect the performance of fog nodes in identifying an infected IoT device. Moreover, the researchers provided a method demonstrating the practical and potential application of preventing the spread of malware in IoT networks.

Al-Hawawreh *et al.* [200] have conducted a comprehensive systematic analysis of ransomware attacks targeting IIoT devices, and suggested several potential defense mechanisms. The authors deployed IIoT devices in an industrial setting following IIRA and analyzed the shortcomings of IIoT environments that might be exploited by ransomware threats. The built test-bed contained I/O devices (i.e., actuators, sensors, and controllers), virtual components (i.e., mail servers, cloud servers, maintenance operators, and SCADA monitoring devices), and IIoT gateways. The authors found that the gateways in the IIoT networks are susceptible to ransomware threats, where IIoT devices and systems might be affected through gateways. The IIoT gateways share some default capabilities;

[12] A mechanism that increases the number of samples of class that has fewer samples; for example, by duplicating the samples of that minority class.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 July 2023 doi:10.20944/preprints202307.0771.v1

they can act as mediators between the outside world and the IIoT environment (i.e., I/O devices or PLCs). Full access to the IIoT gateway can be gained once an attacker initiates a ransomware attack targeting that gateway, changes the legitimate gateway's credentials, and updates the firmware with malignant software. Therefore, the malicious gateway would reveal any data transmitted from users to the external world (or vice-versa). Consequentially, the authors launched ransomware attacks in the considered IIoT environment, utilizing Python scripts similar to the Erebus Linux Ransomware attack. Furthermore, the authors suggested some potential detection and defense mechanisms to protect IIoT environments against ransomware attacks, including the adoption of next-generation firewalls that contain enhanced traffic filtering mechanisms, the utilization of monitoring systems (e.g., IDSs) to detect attacks as early as possible, and the placement of IIoT edge gateways in a trusted zone to prevent infected gateways from affecting the IIoT infrastructure.

Alhawi *et al.* [193] have proposed a decision tree-based approach to detect Windows ransomware network traffic attacks. The proposed framework uses a specialized version of the decision tree, known as J48, and the authors evaluated the method using conversation-based network traffic samples (i.e., packets) along with extracted features (i.e., fields). The proposed framework achieved an acceptable true positive rate of about 97%.

Azmoodeh *et al.* [194] have proposed an approach to detect ransomware attacks targeting IoT networks by measuring the power consumption of Android devices. The proposed method measures various processes to scan energy consumption patterns and differentiate ransomware attacks from legitimate applications. The authors compared four well-known machine learning algorithms (i.e., SVM, neural network, *k*NN, and random forest) using a data set collected from VirusTotal API[13]. The authors conducted various experiments to compare the machine learning algorithms and fine-tune the number of neighbors hyper-parameter, in order to achieve the best result possible. *k*NN with DTW capability achieved the best results, in terms of accuracy, recall, precision, and F1-score, compared to the other machine learning algorithms.

Almashhadani *et al.* [195] have presented a detailed behavioral analysis of activities occurring when crypto-ransomware—particularly, a type of severe ransomware known as Locky—attacks a network. The authors built their own test-bed to validate their assumption. They extracted some important features from the network packets, to classify the captured traffic into various types. Additionally, the authors presented a network-based IDS utilizing two separate detectors working simultaneously at two levels: Flow and packet. Various experiments were conducted using the features extracted by the authors and four machine learning algorithms: Random forest, decision tree, naïve Bayes, and SVM. The proposed technique was shown to be effective in detecting ransomware attacks, through five performance metrics (accuracy, false positive rate, precision, recall, and F1-score), and provided an outstanding detection rate and low false positive rate. The best machine learning algorithm in the packet-based set of experiments was the decision tree, yielding 97.92% accuracy, 97.9% precision, 97.9% recall, 97.9% F1-score, and a false positive rate of 0.021. Meanwhile, the best machine learning algorithm in the flow-based set of experiments was naïve Bayes, which obtained 97.08% accuracy, 0.029 false positive rates, 97.72% precision, 97.71% recall, and 97.71% F1-score.

Maiorca *et al.* [196] have introduced an Android ransomware attack detector using the random forest ensemble method. The proposed technique differs from previous methods, in that it utilizes extracted features from API packages to categorize applications, without needing to be familiar with user-defined content (e.g., strings) and the language used to write the application. The authors evaluated the proposed approach on two public data sets (i.e., the ransomware data set[14] and the malware-trusted data set[15]). The results indicated that the proposed approach is applicable, with very

[13] This data set can be found at the following website: https://www.virustotal.com/gui/home/upload
[14] As indicated by the authors, this data set can be found at http://ransom.mobi/
[15] Found at https://www.sec.cs.tu-bs.de/~danarp/drebin/

 doi:10.20944/preprints202307.0771.v1

high accuracy, to differentiate malware from Android ransomware attacks. Additionally, the authors flagged the detected ransomware applications utilized by the VirusTotal service.

Sgandurra *et al.* [197] have introduced a dynamic analysis and classification approach based on logistic regression, which identifies ransomware threats when users install applications. The introduced method scans some actions executed by applications at the time of installation, in order to detect any indication of ransomware activity. The authors validated the technique on a data set consisting of 583 ransomware samples (downloaded from the VirusShare website) belonging to 11 classes and 942 samples belonging to normal applications. The authors compared their technique with naïve Bayes and SVM. The proposed method was found to be superior to the other methods, in terms of the low complexity of the underline machine learning algorithm and detection rate (achieving 96.3% detection rate and 99.5% ROC curve).

Tseng *et al.* [198] have proposed a DNN-based approach to identify ransomware in a timely manner. The authors presented a labeling mechanism and choose some significant features, in order to improve the performance of the proposed method and reduce the detection time. The proposed method achieved an acceptable detection rate and false negative rate.

8. Opportunities and Future Directions

Individuals and organizations have begun to appreciate the proficiency fog and edge computing paradigms provide to the internet community. This appreciation extends the utilization of these paradigms to store, communicate, and process resources through edge/fog networks instead of CC. The advances of IIoT secure deployment on edge computing were investigated in the previous section. After exploring the progress in the state-of-the-art, there were still some deficiencies in several proposed techniques, hindering the solution of the corresponding security issues. Emerging technologies, such as AI and edge computing, provide various opportunities and issues when integrated to secure IIoT environments. However, the scalability and resilience of edge and fog computing involve various security and privacy challenges [1,201], which may be further investigated by researchers. This section discusses some opportunities and challenges for the secure deployment of IIoT devices at the edge, including secure data sharing, security monitoring, and authentication and access control. This section also presents some insights into how the security of IIoT might be advanced with the help of edge/fog computing and AI in the near future.

8.1. Secure Data Sharing

IIoT devices generate a huge volume of real-time data; thus, data mining enables industries to make the right decisions and inevitably enhance their production efficiency [202]. Traditionally, the design of IIoT is mostly vertically supplied by closed applications, which enable industries to enhance manufacturing processes in a single site. Thus, data islands are forms that need to be split, through the utilization of edge computing, in order to improve their flexibility. Secure data sharing is a complicated issue. Subdividing data islands in an efficient manner and sharing real-time data generated by IIoT devices among heterogeneous applications and entities securely and in a timely manner is expected to become a hot topic related to the IIoT-based edge computing paradigm. Sharing data via edge computing faces two key issues: The limited performance of edge devices, which makes it hard for robust security techniques to be applied, and the unavoidable huge amounts of data, which may lead to more serious consequences (e.g., destruction and cyberattacks). In this context, data generated by IIoT devices in edge computing can be securely shared through the use of a blockchain [203].

If an IIoT device wants to store sensitive data securely, resource-constrained devices such as IIoT devices may not have the storage capacity and processing capability enabling them to store data securely. Thus, edge computing provides IIoT devices with a solution. The edge computing nodes can be equipped with sufficient computational (to deal with complex encryption methods) and storage capabilities, which enable IIoT devices to store data and share data securely. Moreover, edge computing nodes can be distributed close to the IIoT devices, decreasing the associated latency. Even

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 July 2023 doi:10.20944/preprints202307.0771.v1

when big data are generated from IIoT devices (i.e., those which cannot be processed or stored at the edge node), the edge computing node could act as a server to the IIoT devices and a client for cloud computing servers, facilitating data storage and processing (the edge node can also transparently encrypt or decrypt data stored in the cloud server) [204,205]. Therefore, IIoT devices would consider the service to be provided by the edge node and do not need to be aware of the corresponding security or storage methods.

As edge nodes can act as gateways between IIoT devices and external devices, industries can secure and control data flow to and from external devices. By setting up an edge node, high-security standards can be maintained, mutual authentication with outside work can be accomplished, and the limited capacity of IIoT devices can be overcome; hence, IIoT devices only need to process secure communications with edge nodes. Additionally, the edge node can activate the data flow strategy, in order to gain access to the content of the message when processing the traffic passing through it [206].

The distributed service nature of edge and fog computing might lead to data leakage; therefore, it is necessary to prevent unauthorized parties from disclosing stored or in-transit data. Therefore, light encryption techniques such as cryptographic hashing and homomorphic encryption methods could be utilized to protect the transmitted data stored at distributed locations from disclosure. Encrypted data prevents disclosure even if the attacker intercepts the data in transit or accesses secured data stored in specific servers.

Data exchanged between IIoT devices, or between IIoT devices and edge nodes, should be transmitted securely, in order to prevent intruders from modifying or altering the data even if interception occurs. Cryptographic signature verification systems are one of the most notable techniques used to enforce integrity on exchanged data, similar to the GnuPG technique[16], which is utilized to sign transferred data digitally at the sender side and verify it at the receiver side. Data integrity is of paramount significance to IIoT devices when utilizing services on edge computing as, in this situation, the communication between the network entities depends entirely on the network, considering the distributed nature of the network topology.

8.2. Security Monitoring

Edge computing platforms can be equipped with various capabilities, in order to satisfy the needs of IIoT environments. Thus, they may serve as the perfect candidate to be equipped with a substantial system capable of monitoring potential security threats.

An edge node can be equipped with an IDS capable of storing signatures of well-known attacks, thus having the ability to detect intrusions from captured traffic based on these signatures. In the case that the IDS is based on machine learning/deep learning and a number of attack samples need to be used to train the machine learning algorithm, a cloud server could be utilized to train the algorithm, and the weights could be transferred to the edge node for the detection intrusions; hence, the latency issues associated with cloud solutions can be addressed [207].

As sensors communicate their measurements directly to edge nodes, edge nodes can execute anomaly detection mechanisms to ensure that the measurements are within an acceptable range. Therefore, a complete security monitoring system could be deployed to monitor data passing through the edge computing platforms to and from the IIoT environment, allowing for the detection and deterring of threats [208–210]. Additionally, actions can be taken based on traffic passing through, in order to mitigate DoS or DDoS attacks targeting IIoT environments or the edge computing infrastructure.

DoS attacks are one of the biggest issues restraining the availability of services from authorized IIoT devices. These issues could be partially resolved by edge/fog computing, due to the distributed nature of the computational resources. However, DDoS could degrade or prevent authorized IIoT

[16] Found at https://gnupg.org/

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 July 2023 doi:10.20944/preprints202307.0771.v1

devices from accessing these services. IIoT environments could deploy smart DNS resolution services, WAF, and other smart network traffic monitoring and filtering techniques, in order to ensure that services are available at all times.

8.3. Authentication and Access Control

Edge computing can address diverse authentication issues. Edge computing can be applied to replace solutions that necessitate the need for third-party servers [211–215]. An edge node is not resource-constrained and can perform complex computational tasks, consequently having the ability to act as a third-party service to provide IIoT devices with the required authentication mechanism. An advantage of edge nodes over third-party servers is their on-premise placement, providing IIoT devices with low latency when the devices and edge nodes exchange authentication messages. Moreover, an edge node can act as a certificate authority[17] for IIoT devices, thus improving upon conventional PKI infrastructures. Therefore, edge nodes can form a peer-to-peer network to establish a united and powerful key infrastructure [10].

Edge nodes could also serve as trusted gateways, adding new IIoT devices, removing existing ones, and being responsible for re-keying. Some existing works have detailed devices with the required authentication ability through various types of servers, including NFC tags [216–218], smart cards [219–221], RFID tags [222–226], and biometric traits [227–229]. Edge nodes could become a substitute for such a server, and may be attached to sensors, acting as proxies for sensor measurements. In this context, the scalability could be expanded, as more fog nodes may be distributed such that they are reachable by close IIoT devices. Therefore, if there is an urgent need to apply authentication for device updates utilizing NFC keys or biometrics, maintenance engineers would need only the fog node and its binding to the associated key, rather than searching for each device related to the keys independently.

Other authentication capabilities could be brought to IIoT environments through edge computing, such as TPM and TEE. This can be accomplished by setting up a secure communication tunnel between the TEE or TPM and the edge node, as well as adopting a key setup protocol equipped with a one-time pairing feature. Thus, future work is expected to integrate trusted capabilities with edge computing platforms.

Similar to the opportunities related to authentication, access control could be enhanced when integrated with edge computing to authorize IIoT devices. Resource-constrained devices are not the ideal place to carry out access control policies on and, so, these policies could instead be relocated to edge nodes. This would introduce a new issue (i.e., centralization, which might lead to SPOF), as all access control policies would be outsourced from IIoT devices to a specific edge node. A possible solution to this issue is to distribute access control policies through multiple edge nodes, in order to prevent the possibility of SPOF.

IIoT devices share the secure and reliable services provided by edge and fog computing, so mutual trust between IIoT devices and between IIoT devices and edge/fog nodes should be considered. This compels edge and fog servers to prove that the edge nodes that exchange messages with IIoT devices are trustworthy and that their services are genuine. Meanwhile, edge nodes must ensure the authenticity of the IIoT requesting services from edge nodes. These challenges may lead the research community to develop mutual authentication models for IIoT devices and edge nodes utilizing lightweight techniques/devices such as TrustChain [230][18] and PUF [231][19], or developing techniques with low complexity to be deployed in IIoT environments.

---

[17] An organization responsible for signing, storing, and issuing digital certificates.
[18] An authentication scheme based on a permission-less Blockchain network.
[19] An object that provides a physical component with a trust anchor or an unrivaled fingerprint by exploiting the intrinsic randomness introduced during production.

 doi:10.20944/preprints202307.0771.v1

9. Conclusion

As a modern industrial solution, IIoT links network components using advanced communication technologies, helping industries to monitor, exchange, collect and analyze data, thus simplifying crucial decision-making problems, improving productivity, and significantly enhancing performance more than ever. Edge computing can be adopted in the IIoT to process a portion of the large-scale real-time sensing data on the network's edge, near the origin of the data. In this way, the limited transmission bandwidth and long-delay decision-making (i.e., if cloud computing is employed) issues may be resolved. In this survey, a review of IIoT attacks, requirements, and solutions that utilize AI and edge computing, with a focus on the period from 2017 to 2023, was conducted. The security challenges were classified into three categories, based on the IIoT security layer: application layer threats, network layer threats, and perception layer threats. We identified twenty-two attacks that may target these IIoT layers: four attacks targeting the perception layer, eight attacks targeting the network layer, and ten attacks exploiting application vulnerabilities. Each attack was linked with the security requirement it violates and common counter-measures that could be taken to prevent the attack. Additionally, solutions proposed to detect or prevent these attacks and to generally improve the security of IIoT were discussed. Moreover, challenges encountered in the IIoT field when adopting edge computing and AI were detailed, along with the opportunities that these technologies provide. Finally, future research directions were proposed, providing researchers with insights into utilizing AI and edge computing to secure the IIoT paradigm.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The author would like to thank the University of Tabuk for supporting this work.

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

Abbreviations

IoT	Internet of Things
IIoT	Industrial Internet of Things
CPS	Cyber-Physical System
MCC	Mobile Cloud Computing
CC	Cloud Computing
AI	Artificial Intelligence
DDoS	Distributed Denial of Service
IIC	Industrial Internet Consortium
GE	General Electric
AT&T	American Telephone and Telegraph
IBM	International Business Machines
CSP	Cloud Service Provider
ICV	Intelligent Connected Vehicles
CIA	Confidentiality, Integrity, Availability
OTA	Over-The-Air
DoS	Denial of Service
RPL	Routing Protocol for Low-power and lossy networks
SQL	Structured Query Language
SCADA	Supervisory Control And Data Acquisition
ICS	Industrial Control System
WSN	Wireless Sensor Network
IDS	Intrusion Detection System
SSI	Server-Side Injection

 doi:10.20944/preprints202307.0771.v1

XML	eXtensible Markup Language
CSRF	Cross-Site Request Forgery
XSS	Cross-Site Scripting
SSRF	Server-Side Request Forgery
DSI	Device-Side Injection
RCE	Remote Code Execution
ML	Machine Learning
DL	Deep Learning
LSTM	Long Short-Term Memory
SQLI	Structured Query Language Injection
VNF	Virtual Network Function
AES	Advanced Encryption Standard
RSA	Rivest, Shamir, and Adleman
SDN	Software-Defined Networking
VCC	Vehicular Cloud Computing
RNN	Recurrent Neural Network
PKI	Public Key Infrastructure
TPM	Trusted Platform Module
TEE	Trusted Execution Environment
SPOF	Single Point Of Failure
RFID	Radio Frequency Identification
AP	Access Point
Wi-Fi	Wireless Fidelity
PEC	Pervasive Edge Computing
ABC	Artificial Bee Colony
IP	Internet Protocol
RTT	Round Trip Time
IoV	Internet of Vehicles
SVM	Support Vector Machine
ICS	Industrial Control System
FDL	Federated Deep Learning
DNN	Deep Neural Network
PSO	Particle Swarm Optimization
XGBoost	eXtreme Gradient Boosting
MLP	Multi-Layer Perceptron
*k*NN	*k*-Nearest Neighbors
GDE	Global Detection Enactor
GRU	Gated Recurrent Unit
ANN	Artificial Neural Network
HTTP	HyperText Transfer Protocol
LAE	Long short-term memory AutoEncoder
B-LSTM	Bidirectional Long Short-Term Memory
AUC	Area Under the Curve
GM	Geometric Mean
CFBPNN	Cascade Forward Back-Propagation Neural Network
CFS	Correlation-based Feature Selection
NARX	Non-linear Auto-Regressive network with eXogenous inputs
PLC	Program Logic Controller
I/O	Input/Output
IIRA	Industrial Internet Reference Architecture
API	Application Programming Interface
DTW	Dynamic Time Warping
FHSS	Frequency Hopping Spread Spectrum
DSSS	Direct Sequence Spread Spectrum
IPS	Intrusion Prevention System
PUF	Physically Unclonable Functions
GnuPG	GNU Privacy Guard
WAF	Web Application Firewall
DNS	Domain Name System
LR	Logistic Regression
AMI	Advanced Metering Infrastructure
HAN	Home Area Network
MC	Markov Chain

References

1. Chalapathi, G. S. S.; Chamola, V.; Vaish, A.; Buyya, R. Industrial internet of things (iiot) applications of edge and fog computing: A review and future directions. *Fog/edge computing for security, privacy, and applications* **2021**, 293-325.
2. Alotaibi, B. Utilizing blockchain to overcome cyber security concerns in the internet of things: A review. *IEEE Sensors Journal* **2019**, *19(23)*, 10953-10971.
3. Shishehgarkhaneh, M. B.; Moehler, R. C.; Moradinia, S. F. Blockchain in the Construction Industry between 2016 and 2022: A Review, Bibliometric, and Network Analysis. *Smart Cities* **2023**, *6(2)*, 819-845.
4. Ahmad, T.; Zhang, D. Using the internet of things in smart energy systems and networks. *Sustainable Cities and Society* **2021**, *68*, 102783.
5. Tufail, A.; Namoun, A.; Abi Sen, A. A.; Kim, K. H.; Alrehaili, A.; Ali, A. Moisture computing-based internet of vehicles (Iov) architecture for smart cities. *Sensors* **2021**, *21(11)*, 3785.
6. Sisinni, E.; Saifullah, A.; Han, S.; Jennehag, U.; Gidlund, M. Industrial internet of things: Challenges, opportunities, and directions. *IEEE transactions on industrial informatics* **2018**, *14(11)*, 4724-4734.
7. Xu, H.; Yu, W.; Griffith, D.; Golmie, N. A survey on industrial Internet of Things: A cyber-physical systems perspective. *IEEE Access* **2018**, *6*, 78238-78259.
8. Basir, R.; Qaisar, S.; Ali, M.; Aldwairi, M.; Ashraf, M. I.; Mahmood, A.; Gidlund, M. Fog computing enabling industrial internet of things: State-of-the-art and research challenges. *Sensors* **2019**, *19(21)*, 4807.
9. Stefanescu, D.; Galán-García, P.; Montalvillo, L.; Unzilla, J.; Urbieta, A. Industrial Data Homogenization and Monitoring Scheme with Blockchain Oracles. *Smart Cities* **2023**, *6(1)*, 263-290.
10. Tange, K.; De Donno, M.; Fafoutis, X.; Dragoni, N. A systematic survey of industrial Internet of Things security: Requirements and fog computing opportunities. *IEEE Communications Surveys & Tutorials* **2020**, *22(4)*, 2489-2520.
11. Daugherty, P.; Berthon, B. (2015). Winning with the industrial internet of things: How to accelerate the journey to productivity and growth. Dublín: Accenture.
12. Rabbani, M. M.; Dushku, E.; Vliegen, J.; Braeken, A.; Dragoni, N.; Mentens, N. (2021, November). Reserve: Remote attestation of intermittent iot devices. In Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems (pp. 578-580).
13. Fernández-Carrasco, J. Á.; Echeberria-Barrio, X.; Paredes-García, D., Zola, F.; Orduna-Urrutia, R. ChronoEOS 2.0: Device Fingerprinting and EOSIO Blockchain Technology for On-Running Forensic Analysis in an IoT Environment. *Smart Cities* **2023**, *6(2)*, 897-912.
14. Xenofontos, C.; Zografopoulos, I.; Konstantinou, C.; Jolfaei, A.; Khan, M. K.; Choo, K. K. R. (2021). Consumer, commercial, and industrial iot (in) security: Attack taxonomy and case studies. IEEE Internet of Things Journal, 9(1), 199-221.
15. Ferrag, M. A.; Friha, O.; Hamouda, D.; Maglaras, L.; Janicke, H. Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning. *IEEE Access* **2022**, *10*, 40281-40306.
16. Botta, A.; De Donato, W.; Persico, V.; Pescapé, A. Integration of cloud computing and internet of things: a survey. *Future generation computer systems* **2016**, *56*, 684-700.
17. Díaz, M.; Martín, C.; Rubio, B. State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing. *Journal of Network and Computer applications* **2016**, *67*, 99-117.
18. Javadzadeh, G.; Rahmani, A. M. Fog computing applications in smart cities: A systematic survey. *Wireless Networks* **2020**, *26(2)*, 1433-1457.
19. Hussain, M. M., & Beg, M. S. (2019). Fog computing for internet of things (IoT)-aided smart grid architectures. Big Data and cognitive computing, 3(1), 8.
20. Alzoubi, Y. I.; Osmanaj, V. H.; Jaradat, A.; Al-Ahmad, A. Fog computing security and privacy for the Internet of Thing applications: State-of-the-art. *Security and Privacy* **2021**, *4(2)*, e145.
21. Qiu, T., Chi, J., Zhou, X., Ning, Z., Atiquzzaman, M., & Wu, D. O. (2020). Edge computing in industrial internet of things: Architecture, advances and challenges. IEEE Communications Surveys & Tutorials, 22(4), 2462-2488.
22. Touqeer, H.; Zaman, S.; Amin, R.; Hussain, M.; Al-Turjman, F.; Bilal, M. Smart home security: challenges, issues and solutions at different IoT layers. *The Journal of Supercomputing* **2021**, *77(12)*, 14053-14089.

23. Hazra, A.; Adhikari, M.; Amgoth, T.; Srirama, S. N. A comprehensive survey on interoperability for IIoT: Taxonomy, standards, and future directions. *ACM Computing Surveys (CSUR)* **2021**, *55(1)*, 1-35.
24. Alguliyev, R.; Imamverdiyev, Y.; Sukhostat, L. Cyber-physical systems and their security issues. *Computers in Industry* **2018**, *100*, 212-223.
25. Ortiz, A. M.; Hussein, D.; Park, S.; Han, S. N.; Crespi, N. The cluster between internet of things and social networks: Review and research challenges. *IEEE Internet of Things Journal* **2014**, *1(3)*, 206-215.
26. Pivoto, D. G.; de Almeida, L. F.; da Rosa Righi, R.; Rodrigues, J. J.; Lugli, A. B.; Alberti, A. M. Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review. *Journal of manufacturing systems* **2021**, *58*, 176-192.
27. Nunes, D. S.; Zhang, P.; Silva, J. S. A survey on human-in-the-loop applications towards an internet of all. *IEEE Communications Surveys & Tutorials* **2015**, *17(2)*, 944-965.
28. Stojmenovic, I. Machine-to-machine communications with in-network data aggregation, processing, and actuation for large-scale cyber-physical systems. *IEEE Internet of Things Journal* **2014**, *1(2)*, 122-128.
29. Dai, Y.; Guan, Y. L.; Leung, K. K.; Zhang, Y. Reconfigurable intelligent surface for low-latency edge computing in 6G. *IEEE Wireless Communications* **2021**, *28(6)*, 72-79.
30. Gasmi, K.; Dilek, S.; Tosun, S.; Ozdemir, S. A survey on computation offloading and service placement in fog computing-based IoT. *The Journal of Supercomputing* **2022**, *78(2)*, 1983-2014.
31. Sofla, M. S.; Kashani, M. H.; Mahdipour, E.; Mirzaee, R. F. Towards effective offloading mechanisms in fog computing. *Multimedia Tools and Applications* **2022**, *81(2)*, 1997.
32. Meneghello, F.; Calore, M.; Zucchetto, D.; Polese, M.; Zanella, A. IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet of Things Journal* **2019**, *6(5)*, 8182-8201.
33. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations. *IEEE Communications Surveys & Tutorials* **2019**, *21(3)*, 2702-2733.
34. Kouicem, D. E.; Bouabdallah, A.; Lakhlef, H. Internet of things security: A top-down survey. *Computer Networks* **2018**, *141*, 199-221.
35. Lezzi, M.; Lazoi, M.; Corallo, A. Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers in Industry* **2018**, *103*, 97-110.
36. Hofer, F. (2018, October). Architecture, technologies and challenges for cyber-physical systems in industry 4.0: A systematic mapping study. In Proceedings of the 12th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (pp. 1-10).
37. Hansch, G.; Schneider, P.; Fischer, K.; Böttinger, K. (2019, September). A unified architecture for industrial IoT security requirements in open platform communications. In 2019 24th ieee international conference on emerging technologies and factory automation (etfa) (pp. 325-332). IEEE.
38. 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 Fransisco, California, 07–11 June 2015; pp. 1–6.
39. Sajid, A.; Abbas, H.; Saleem, K. Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. *IEEE Access* **2016**, *4*, 1375-1384.
40. Tan, S. F.; Samsudin, A. Recent technologies, security countermeasure and ongoing challenges of Industrial Internet of Things (IIoT): A survey. *Sensors* **2021**, *21(19)*, 6647.
41. Ni, J.; Lin, X.; Shen, X. S. Toward edge-assisted Internet of Things: From security and efficiency perspectives. *IEEE Network* **2019**, *33(2)*, 50-57.
42. Guan, Y.; Shao, J.; Wei, G.; Xie, M. Data security and privacy in fog computing. *IEEE Network* **2018**, *32(5)*, 106-111.
43. Zhang, J.; Chen, B.; Zhao, Y.; Cheng, X.; Hu, F. Data security and privacy-preserving in edge computing paradigm: Survey and open issues. *IEEE Access* **2018**, *6*, 18209-18237.
44. Georgakopoulos, D.; Jayaraman, P. P.; Fazia, M.; Villari, M.; Ranjan, R. Internet of Things and edge cloud computing roadmap for manufacturing. *IEEE Cloud Computing* **2016**, *3(4)*, 66-73.
45. Seitz, A.; Buchinger, D.; Bruegge, B. (2018, March). The conjunction of fog computing and the industrial internet of things-an applied approach. In 2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) (pp. 812-817). IEEE.

46. Sittón-Candanedo, I.; Alonso, R. S.; Rodríguez-González, S.; García Coria, J. A.; De La Prieta, F. (2020). Edge computing architectures in industry 4.0: A general survey and comparison. In 14th International Conference on Soft Computing Models in Industrial and Environmental Applications (SOCO 2019) Seville, Spain, May 13–15, 2019, Proceedings 14 (pp. 121-131). Springer International Publishing.
47. Steiner, W.; Poledna, S. Fog computing as enabler for the Industrial Internet of Things. *Elektrotechnik und Informationstechnik* **2016**, *133(7)*, 310-314.
48. Aazam, M.; Zeadally, S.; Harras, K. A. Deploying fog computing in industrial internet of things and industry 4.0. *IEEE Transactions on Industrial Informatics* **2018**, *14(10)*, 4674-4682.
49. Hassanzadeh, A.; Modi, S.; Mulchandani, S. (2015, December). Towards effective security control assignment in the Industrial Internet of Things. In 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT) (pp. 795-800). IEEE.
50. Ferrag, M. A.; Maglaras, L. A.; Janicke, H., Jiang, J.; Shu, L. Authentication protocols for internet of things: a comprehensive survey. *Security and Communication Networks* **2017**, *2017*.
51. Pereira, T.; Barreto, L.; Amaral, A. Network and information security challenges within Industry 4.0 paradigm. *Procedia manufacturing* **2017**, *13*, 1253-1260.
52. Khurshid, A., Khan, A. N., Khan, F. G., Ali, M., Shuja, J., & Khan, A. U. R. (2019). Secure-CamFlow: a device-oriented security model to assist information flow control systems in cloud environments for IoTs. Concurrency and Computation: Practice and Experience, 31(8), e4729.
53. Dammak, M.; Boudia, O. R. M.; Messous, M. A.; Senouci, S. M.; Gransart, C. (2019, January). Token-based lightweight authentication to secure IoT networks. In 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC) (pp. 1-4). IEEE.
54. Falco, G.; Caldera, C.; Shrobe, H. IIoT cybersecurity risk modeling for SCADA systems. *IEEE Internet of Things Journal* **2018**, *5(6)*, 4486-4495.
55. Riad, K.; Hamza, R.; Yan, H. Sensitive and energetic IoT access control for managing cloud electronic health records. *IEEE Access* **2019**, *7*, 86384-86393.
56. Hameed, S.; Khan, F. I.; Hameed, B. Understanding security requirements and challenges in Internet of Things (IoT): A review. *Journal of Computer Networks and Communications* **2019**, *2019*, 1-14.
57. Wu, H.; Miao, Y.; Zhang, P.; Tian, Y.; Tian, H. Resilience in Industrial Internet of Things Systems: A Communication Perspective. *arXiv preprint* **2022** arXiv:2206.00217.
58. Laszka, A.; Abbas, W.; Vorobeychik, Y.; Koutsoukos, X. (2018, October). Synergistic security for the industrial internet of things: Integrating redundancy, diversity, and hardening. In 2018 IEEE International Conference on Industrial Internet (ICII) (pp. 153-158). IEEE.
59. Zhou, L.; Guo, H. (2018, July). Anomaly detection methods for IIoT networks. In 2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI) (pp. 214-219). IEEE.
60. Bakhshi, Z.; Balador, A.; Mustafa, J. (2018, April). Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models. In 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW) (pp. 173-178). IEEE.
61. Solangi, Z. A.; Solangi, Y. A.; Chandio, S.; bin Hamzah, M. S.; Shah, A. (2018, May). The future of data privacy and security concerns in Internet of Things. In 2018 IEEE International Conference on Innovative Research and Development (ICIRD) (pp. 1-4). IEEE.
62. Khan, W. Z.; Aalsalem, M. Y.; Khan, M. K. Communal acts of IoT consumers: A potential threat to security and privacy. *IEEE Transactions on Consumer Electronics* **2018**, *65(1)*, 64-72.
63. Zhou, L.; Yeh, K. H.; Hancke, G.; Liu, Z.; Su, C. Security and privacy for the industrial internet of things: An overview of approaches to safeguarding endpoints. *IEEE Signal Processing Magazine* **2018**, *35(5)*, 76-87.
64. Settanni, G.; Skopik, F.; Karaj, A.; Wurzenberger, M.; Fiedler, R. (2018, May). Protecting cyber physical production systems using anomaly detection to enable self-adaptation. In 2018 IEEE Industrial Cyber-Physical Systems (ICPS) (pp. 173-180). IEEE.
65. Zolanvari, M.; Teixeira, M. A.; Jain, R. (2018, November). Effect of imbalanced datasets on security of industrial IoT using machine learning. In 2018 IEEE international conference on intelligence and security informatics (ISI) (pp. 112-117). IEEE.
66. Zugasti, E.; Iturbe, M.; Garitano, I.; Zurutuza, U. (2018, June). Null is not always empty: Monitoring the null space for field-level anomaly detection in industrial IoT environments. In 2018 Global Internet of Things Summit (GIoTS) (pp. 1-6). IEEE.

67. Elrawy, M. F.; Awad, A. I.; Hamed, H. F. Intrusion detection systems for IoT-based smart environments: a survey. *Journal of Cloud Computing* **2018**, *7(1)*, 1-20.
68. Rubio-Loyola, J.; Sala, D.; Ali, A. I. (2008, October). Accurate real-time monitoring of bottlenecks and performance of packet trace collection. In 2008 33rd IEEE Conference on Local Computer Networks (LCN) (pp. 884-891). IEEE.
69. Rubio-Loyola, J.; Sala, D.; Ali, A. I. (2008, September). Maximizing packet loss monitoring accuracy for reliable trace collections. In 2008 16th IEEE workshop on local and metropolitan area networks (pp. 61-66). IEEE.
70. Ghorbani, A. A.; Lu, W.; Tavallaee, M. Network Intrusion Detection and Prevention, *Advances in Information Security* **2010**. Inf. Syst, 223.
71. Anwar, S.; Mohamad Zain, J.; Zolkipli, M. F.; Inayat, Z.; Khan, S.; Anthony, B.; Chang, V. From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions. *Algorithms* **2017**, *10(2)*, 39.
72. Bul'ajoul, W.; James, A.; Pannu, M. Improving network intrusion detection system performance through quality of service configuration and parallel technology. *Journal of Computer and System Sciences* **2015**, *81(6)*, 981-999.
73. Meng, W.; Li, W.; Kwok, L. F. EFM: enhancing the performance of signature-based network intrusion detection systems using enhanced filter mechanism. *computers & security* **2014**, *43*, 189-204.
74. Abduvaliyev, A.; Pathan, A. S. K.; Zhou, J.; Roman, R.; Wong, W. C. On the vital areas of intrusion detection systems in wireless sensor networks. *IEEE Communications Surveys & Tutorials* **2013**, *15(3)*, 1223-1237.
75. Nisioti, A.; Mylonas, A.; Yoo, P. D.; Katos, V. From intrusion detection to attacker attribution: A comprehensive survey of unsupervised methods. *IEEE Communications Surveys & Tutorials* **2018**, *20(4)*, 3369-3388.
76. Bhuyan, M. H.; Bhattacharyya, D. K.; Kalita, J. K. Network anomaly detection: methods, systems and tools. *IEEE Communications Surveys & Tutorials* **2013**, *16(1)*, 303-336.
77. Hong, J.; Liu, C. C.; Govindarasu, M. Integrated anomaly detection for cyber security of the substations. *IEEE Transactions on Smart Grid* **2014**, *5(4)*, 1643-1653.
78. Mishra, P.; Pilli, E. S.; Varadharajan, V.; Tupakula, U. Intrusion detection techniques in cloud environment: A survey. *Journal of Network and Computer Applications* **2017**, *77*, 18-47.
79. Lesjak, C.; Ruprechter, T.; Bock, H.; Haid, J.; Brenner, E. (2014, December). ESTADO—Enabling smart services for industrial equipment through a secured, transparent and ad-hoc data transmission online. In The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014) (pp. 171-177). IEEE.
80. Autenrieth, P.; Lörcher, C.; Pfeiffer, C.; Winkens, T.; Martin, L. (2018, June). Current significance of IT-infrastructure enabling industry 4.0 in large companies. In 2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC) (pp. 1-8). IEEE.
81. Jazdi, N. (2014, May). Cyber physical systems in the context of Industry 4.0. In 2014 IEEE international conference on automation, quality and testing, robotics (pp. 1-4). IEEE.
82. Moyne, J.; Mashiro, S.; Gross, D. (2018, April). Determining a security roadmap for the microelectronics industry. In 2018 29th Annual SEMI Advanced Semiconductor Manufacturing Conference (ASMC) (pp. 291-294). IEEE.
83. Benias, N.; Markopoulos, A. P. (2017, September). A review on the readiness level and cyber-security challenges in Industry 4.0. In 2017 South Eastern European Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM) (pp. 1-5). IEEE.
84. Drias, Z.; Serhrouchni, A.; Vogel, O. (2015, August). Analysis of cyber security for industrial control systems. In 2015 international conference on cyber security of smart cities, industrial control system and communications (ssic) (pp. 1-8). IEEE.
85. Oztemel, E.; Gursev, S. Literature review of Industry 4.0 and related technologies. *Journal of intelligent manufacturing* **2020**, *31*, 127-182.
86. Zhou, K.; Liu, T.; Zhou, L. (2015, August). Industry 4.0: Towards future industrial opportunities and challenges. In 2015 12th International conference on fuzzy systems and knowledge discovery (FSKD) (pp. 2147-2152). IEEE.

87. Putra, F. A.; Ramli, K.; Hayati, N.; Gunawan, T. S. PURA-SCIS protocol: A novel solution for cloud-based information sharing protection for sectoral organizations. *Symmetry* **2021**, *13(12)*, 2347.
88. Esposito, C.; Castiglione, A.; Martini, B.; Choo, K. K. R. Cloud manufacturing: security, privacy, and forensic concerns. *IEEE Cloud Computing* **2016**, *3(4)*, 16-22.
89. Abba Ari, A. A.; Ngangmo, O. K.; Titouna, C.; Thiare, O.; Mohamadou, A.; Gueroui, A. M. Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges. *Applied Computing and Informatics* **2020**.
90. Abosata, N.; Al-Rubaye, S.; Inalhan, G.; Emmanouilidis, C. Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications. *Sensors* **2021**, *21(11)*, 3654.
91. Chakrabarty, S.; Engels, D. W.; Thathapudi, S. (2015, October). Black SDN for the Internet of Things. In 2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems (pp. 190-198). IEEE.
92. Lakshminarayana, S.; Karachiwala, J. S.; Chang, S. Y.; Revadigar, G.; Kumar, S. L. S.; Yau, D. K.; Hu, Y. C. (2018, June). Signal jamming attacks against communication-based train control: Attack impact and countermeasure. In Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks (pp. 160-171).
93. Aarika, K.; Bouhlal, M.; Abdelouahid, R. A.; Elfilali, S.; Benlahmar, E. Perception layer security in the internet of things. *Procedia Computer Science* **2020**, *175*, 591-596.
94. Abdul-Ghani, H. A.; Konstantas, D. A comprehensive study of security and privacy guidelines, threats, and countermeasures: An IoT perspective. *Journal of Sensor and Actuator Networks* **2019**, *8(2)*, 22.
95. Farha, F.; Ning, H.; Yang, S.; Xu, J.; Zhang, W.; Choo, K. K. R. Timestamp scheme to mitigate replay attacks in secure ZigBee networks. *IEEE Transactions on Mobile Computing* **2020**, *21(1)*, 342-351.
96. Grammatikis, P. I. R.; Sarigiannidis, P. G.; Moscholios, I. D. Securing the Internet of Things: Challenges, threats and solutions. *Internet of Things* **2019**, *5*, 41-70.
97. Hasan, M. K.; Ghazal, T. M.; Saeed, R. A.; Pandey, B.; Gohel, H.; Eshmawi, A. A., ... ; Alkhassawneh, H. M. A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things. *IET Communications* **2022**, *16(5)*, 421-432.
98. Kaliyar, P.; Jaballah, W. B.; Conti, M.; Lal, C. LiDL: localization with early detection of sybil and wormhole attacks in IoT networks. *Computers & Security* **2020**, *94*, 101849.
99. Patel, M.; Aggarwal, A.; Chaubey, N. Wormhole attacks and countermeasures in wireless sensor networks: a survey. *International Journal of Engineering and Technology (IJET)* **2017**, ISSN, 0975-4024.
100. Djuitcheu, H.; Debes, M.; Aumüller, M.; Seitz, J. (2022, March). Recent review of distributed denial of service attacks in the internet of things. In 2022 5th Conference on Cloud and Internet of Things (CIoT) (pp. 32-39). IEEE.
101. Tsiknas, K.; Taketzis, D.; Demertzis, K.; Skianis, C. Cyber threats to industrial IoT: a survey on attacks and countermeasures. *IoT* **2021**, *2(1)*, 163-186.
102. Sharma, M.; Bhushan, B.; Khamparia, A. (2021). Securing Internet of Things: attacks, countermeasures and open challenges. In Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2020, Volume 1 (pp. 873-885). Springer Singapore.
103. Sharma, G.; Vidalis, S.; Anand, N.; Menon, C.; Kumar, S. A survey on layer-wise security attacks in IoT: Attacks, countermeasures, and open-issues. *Electronics* **2021**, *10(19)*, 2365.
104. Butun, I.; Österberg, P.; Song, H. Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. *IEEE Communications Surveys & Tutorials* **2019**, *22(1)*, 616-644.
105. Bagga, M.; Thakral, P.; Bagga, T. (2018, December). A Study on IoT: Model, Communication Protocols, Security Hazards & Countermeasures. In 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC) (pp. 591-598). IEEE.
106. Rodríguez, G. E.; Torres, J. G.; Flores, P.; Benavides, D. E. Cross-site scripting (XSS) attacks and mitigation: A survey. *Computer Networks* **2020**, *166*, 106960.
107. Prabhavathy, M.; Umamaheswari, S. Prevention of Runtime Malware Injection Attack in Cloud Using Unsupervised Learning. *Intelligent Automation & Soft Computing* **2022**, *32(1)*.
108. Xing, K.; Srinivasan, S. S. R.; Rivera, M. J. M.; Li, J.; Cheng, X. Attacks and countermeasures in sensor networks: a survey. *Network security* **2010**, 251-272.

109. Halfond, W. G.; Viegas, J.; Orso, A. (2006, March). A classification of SQL-injection attacks and countermeasures. In Proceedings of the IEEE international symposium on secure software engineering (Vol. 1, pp. 13-15). IEEE.
110. Silva, J. A. H.; López, L. I. B.; Caraguay, Á. L. V.; Hernández-Álvarez, M. A survey on situational awareness of ransomware attacks—detection and prevention parameters. *Remote Sensing* **2019**, *11(10)*.
111. Spreitzer, R.; Moonsamy, V.; Korak, T.; Mangard, S. Systematic classification of side-channel attacks: A case study for mobile devices. *IEEE communications surveys & tutorials* **2017**, *20(1)*, 465-488.
112. Jesudoss, A.; Subramaniam, N. A survey on authentication attacks and countermeasures in a distributed environment. *Indian Journal of Computer Science and Engineering (IJCSE)* **2014**, *5(2)*, 71-77.
113. Deogirikar, J.; Vidhate, A. (2017, February). Security attacks in IoT: A survey. In 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 32-37). IEEE.
114. Kumar, S.; Sahoo, S.; Mahapatra, A.; Swain, A. K.; Mahapatra, K. K. (2017, December). Security enhancements to system on chip devices for IoT perception layer. In 2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS) (pp. 151-156). IEEE.
115. Ingham, M.; Marchang, J.; Bhowmik, D. IoT security vulnerabilities and predictive signal jamming attack analysis in LoRaWAN. *IET information security* **2020**, *14(4)*, 368-379.
116. Ahmad, I.; Niazy, M. S.; Ziar, R. A.; Khan, S. Survey on IoT: security threats and applications. *Journal of Robotics and Control (JRC)* **2021**, *2(1)*, 42-46.
117. Kalinin, E.; Belyakov, D.; Bragin, D.; Konev, A. IoT Security Mechanisms in the Example of BLE. *Computers* **2021**, *10(12)*, 162.
118. Kakkar, L.; Gupta, D.; Saxena, S.; Tanwar, S. (2021). IoT architectures and its security: a review. In Proceedings of the Second International Conference on Information Management and Machine Intelligence: ICIMMI 2020 (pp. 87-94). Springer Singapore.
119. Wallgren, L.; Raza, S.; Voigt, T. Routing attacks and countermeasures in the RPL-based internet of things. *International Journal of Distributed Sensor Networks* **2013**, *9(8)*, 794326.
120. Ding, J.; Zhang, H.; Guo, Z.; Wu, Y. The DPC-based scheme for detecting selective forwarding in clustered wireless sensor networks. *IEEE Access* **2021**, *9*, 20954-20967.
121. Shah, Y.; Sengupta, S. (2020, October). A survey on Classification of Cyber-attacks on IoT and IIoT devices. In 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 0406-0413). IEEE.
122. de Oliveira, G. H.; de Souza Batista, A.; Nogueira, M.; dos Santos, A. L. An access control for IoT based on network community perception and social trust against Sybil attacks. *International Journal of Network Management* **2022**, *32(1)*, e2181.
123. Morales-Molina, C. D.; Hernandez-Suarez, A.; Sanchez-Perez, G.; Toscano-Medina, L. K.; Perez-Meana, H.; Olivares-Mercado, J.; ... Garcia-Villalba, L. J. A dense neural network approach for detecting clone id attacks on the rpl protocol of the iot. *Sensors* **2021**, *21(9)*, 3173.
124. Pongle, P.; Chavan, G. (2015, January). A survey: Attacks on RPL and 6LoWPAN in IoT. In 2015 International conference on pervasive computing (ICPC) (pp. 1-6). IEEE.
125. Kamaleshwar, T.; Lakshminarayanan, R.; Teekaraman, Y.; Kuppusamy, R.; Radhakrishnan, A. Self-adaptive framework for rectification and detection of black hole and wormhole attacks in 6lowpan. *Wireless Communications and Mobile Computing* **2021**, *2021*, 1-8.
126. Bhosale, S. A.; Sonavane, S. S. Wormhole attack detection system for IoT network: A hybrid approach. *Wireless Personal Communications* **2022**, *124(2)*, 1081-1108.
127. Adefemi Alimi, K. O., Ouahada, K., Abu-Mahfouz, A. M., Rimer, S., & Alimi, O. A. (2022). Refined LSTM based intrusion detection for denial-of-service attack in Internet of Things. Journal of sensor and actuator networks, 11(3), 32.
128. Jazzar, M.; Hamad, M. (2022, January). An Analysis Study of IoT and DoS Attack Perspective. In Proceedings of International Conference on Intelligent Cyber-Physical Systems: ICPS 2021 (pp. 127-142). Singapore: Springer Nature Singapore.
129. Narayanan, A.; De Sena, A. S.; Gutierrez-Rojas, D.; Melgarejo, D. C.; Hussain, H. M.; Ullah, M.; ... ; Nardelli, P. H. Key advances in pervasive edge computing for industrial internet of things in 5g and beyond. *IEEE Access* **2020**, *8*, 206734-206754.

130. Bhardwaj, K.; Miranda, J. C.; Gavrilovska, A. (2018). Towards IoT-DDoS Prevention Using Edge Computing. In USENIX workshop on hot topics in edge computing (HotEdge 18).
131. Zhou, L.; Guo, H.; Deng, G. A fog computing based approach to DDoS mitigation in IIoT systems. *Computers & Security* **2019**, *85*, 51-62.
132. Antonakakis, M.; April, T.; Bailey, M.; Bernhard, M.; Bursztein, E.; Cochran, J.; ... Zhou, Y. (2017). Understanding the mirai botnet. In 26th USENIX security symposium (USENIX Security 17) (pp. 1093-1110).
133. Abdul-Ghani, H. A.; Konstantas, D.; Mahyoub, M. A comprehensive IoT attacks survey based on a building-blocked reference model. *International Journal of Advanced Computer Science and Applications* **2018**, *9(3)*, 355-373.
134. Ioannou, C.; Vassiliou, V. Network attack classification in IoT using support vector machines. *Journal of sensor and actuator networks* **2021**, *10(3)*, 58.
135. Ioulianou, P. P.; Vassilakis, V. G.; Shahandashti, S. F. A trust-based intrusion detection system for RPL networks: Detecting a combination of rank and blackhole attacks. *Journal of Cybersecurity and Privacy* **2022**, *2(1)*, 124-153.
136. Donta, P. K.; Srirama, S. N.; Amgoth, T.; Annavarapu, C. S. R. Survey on recent advances in IoT application layer protocols and machine learning scope for research directions. *Digital Communications and Networks* **2022**, *8(5)*, 727-744.
137. Abdullah, A.; Hamad, R.; Abdulrahman, M.; Moala, H.; Elkhediri, S. (2019, May). CyberSecurity: a review of internet of things (IoT) security issues, challenges and techniques. In 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-6). IEEE.
138. Acar, G.; Huang, D. Y.; Li, F., Narayanan, A.; Feamster, N. (2018, August). Web-based attacks to discover and control local IoT devices. In Proceedings of the 2018 Workshop on IoT Security and Privacy (pp. 29-35).
139. Watson, M. R.; Marnerides, A. K.; Mauthe, A.; Hutchison, D. Malware detection in cloud computing infrastructures. *IEEE Transactions on Dependable and Secure Computing* **2015**, *13(2)*, 192-205.
140. Barron, C.; Yu, H.; Zhan, J. (2013, July). Cloud computing security case studies and research. In Proceedings of the world congress on engineering (Vol. 2, No. 2, pp. 1-6).
141. Xiao, Y.; Jia, Y.; Liu, C.; Cheng, X.; Yu, J.; Lv, W. Edge computing security: State of the art and challenges. *Proceedings of the IEEE* **2019**, *107(8)*, 1608-1631.
142. Gautam, S.; Malik, A.; Singh, N.; Kumar, S. (2019, March). Recent advances and countermeasures against various attacks in IoT environment. In 2019 2nd international conference on signal processing and communication (ICSPC) (pp. 315-319). IEEE.
143. Zolanvari, M.; Teixeira, M. A.; Gupta, L.; Khan, K. M.; Jain, R. Machine learning-based network vulnerability analysis of industrial Internet of Things. *IEEE Internet of Things Journal* **2019**, *6(4)*, 6822-6834.
144. Humayun, M.; Jhanjhi, N. Z.; Alsayat, A.; Ponnusamy, V. Internet of things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal* **2021**, *22(1)*, 105-117.
145. Xu, Y.; Cui, W.; Peinado, M. (2015, May). Controlled-channel attacks: Deterministic side channels for untrusted operating systems. In 2015 IEEE Symposium on Security and Privacy (pp. 640-656). IEEE.
146. Zhang, T.; Zhang, Y.; Lee, R. B. (2016). Cloudradar: A real-time side-channel attack detection system in clouds. In Research in Attacks, Intrusions, and Defenses: 19th International Symposium, RAID 2016, Paris, France, September 19-21, 2016, Proceedings 19 (pp. 118-140). Springer International Publishing.
147. Lyu, Y.; Mishra, P. A survey of side-channel attacks on caches and countermeasures. *Journal of Hardware and Systems Security* **2018**, *2*, 33-50.
148. Ansari, M. S.; Alsamhi, S. H.; Qiao, Y.; Ye, Y.; Lee, B. (2020). Security of distributed intelligence in edge computing: Threats and countermeasures. The Cloud-to-Thing Continuum: Opportunities and Challenges in Cloud, Fog and Edge Computing, 95-122.
149. Alkhwaja, I.; Albugami, M.; Alkhwaja, A.; Alghamdi, M.; Abahussain, H.; Alfawaz, F.; ... Min-Allah, N. Password Cracking with Brute Force Algorithm and Dictionary Attack Using Parallel Programming. *Applied Sciences* **2023**, *13(10)*, 5979.
150. Zuin, N. K.; Selvarajah, V. (2021, September). A Case Study: SYN Flood Attack Launched Through Metasploit. In 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021) (pp. 520-525). Atlantis Press.
151. Qiu, T.; Liu, J.; Si, W.; Wu, D. O. Robustness optimization scheme with multi-population co-evolution for scale-free wireless sensor networks. *IEEE/ACM Transactions on Networking* **2019**, *27(3)*, 1028-1042.

152. Diro, A.; Chilamkurti, N. Leveraging LSTM networks for attack detection in fog-to-things communications. *IEEE Communications Magazine* **2018**, *56(9)*, 124-130.
153. Chekired, D. A.; Khoukhi, L.; Mouftah, H. T. (2019, May). Fog-based distributed intrusion detection system against false metering attacks in smart grid. In ICC 2019-2019 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.
154. Huang, H.; Ye, P.; Hu, M.; Wu, J. A multi-point collaborative DDoS defense mechanism for IIoT environment. *Digital Communications and Networks* **2023**, *9(2)*, 590-601.
155. Mudassir, M.; Unal, D.; Hammoudeh, M.; Azzedin, F. Detection of botnet attacks against industrial IoT systems by multilayer deep learning approaches. *Wireless Communications and Mobile Computing* **2022**, *2022*.
156. Tsogbaatar, E.; Bhuyan, M. H.; Taenaka, Y.; Fall, D.; Gonchigsumlaa, K.; Elmroth, E.; Kadobayashi, Y. DeL-IoT: A deep ensemble learning approach to uncover anomalies in IoT. *Internet of Things* **2021**, *14*, 100391.
157. Popoola, S. I.; Adebisi, B.; Hammoudeh, M.; Gui, G.; Gacanin, H. Hybrid deep learning for botnet attack detection in the internet-of-things networks. *IEEE Internet of Things Journal* **2020**, *8(6)*, 4944-4956.
158. Popoola, S. I.; Adebisi, B.; Ande, R.; Hammoudeh, M.; Anoh, K.; Atayero, A. A. smote-drnn: A deep learning algorithm for botnet detection in the internet-of-things networks. *Sensors* **2021**, *21(9)*, 2985.
159. Jayalaxmi, P. L. S.; Kumar, G.; Saha, R.; Conti, M.; Kim, T. H.; Thomas, R. DeBot: A deep learning-based model for bot detection in industrial internet-of-things. *Computers and Electrical Engineering* **2022**, *102*, 108214.
160. Alani, M. M. BotStop: Packet-based efficient and explainable IoT botnet detection using machine learning. *Computer Communications* **2022**, *193*, 53-62.
161. Popoola, S. I.; Ande, R.; Adebisi, B.; Gui, G.; Hammoudeh, M.; Jogunola, O. Federated deep learning for zero-day botnet attack detection in IoT-edge devices. *IEEE Internet of Things Journal* **2021**, *9(5)*, 3930-3944.
162. Li, J.; Lyu, L.; Liu, X.; Zhang, X.; Lyu, X. FLEAM: A federated learning empowered architecture to mitigate DDoS in industrial IoT. *IEEE Transactions on Industrial Informatics* **2021**, *18(6)*, 4059-4068.
163. Wazid, M.; Reshma Dsouza, P.; Das, A. K.; Bhat K, V.; Kumar, N.; Rodrigues, J. J. RAD-EI: A routing attack detection scheme for edge-based Internet of Things environment. *International Journal of Communication Systems* **2019**, *32(15)*, e4024.
164. Singh, T.; Aksanli, B. (2019, November). Real-time traffic monitoring and SQL injection attack detection for edge networks. In Proceedings of the 15th ACM International Symposium on QoS and Security for Wireless and Mobile Networks (pp. 29-36).
165. Yan, Q.; Huang, W.; Luo, X.; Gong, Q.; Yu, F. R. A multi-level DDoS mitigation framework for the industrial Internet of Things. *IEEE Communications Magazine* **2018**, *56(2)*, 30-36.
166. Simpson, S. V.; Nagarajan, G. A fuzzy based co-operative blackmailing attack detection scheme for edge computing nodes in MANET-IOT environment. *Future Generation Computer Systems* **2021**, *125*, 544-563.
167. Zaminkar, M.; Fotohi, R. SoS-RPL: securing internet of things against sinkhole attack using RPL protocol-based node rating and ranking mechanism. *Wireless Personal Communications* **2020**, *114(2)*, 1287-1312.
168. Khan, F.; Jan, M. A.; ur Rehman, A.; Mastorakis, S.; Alazab, M.; Watters, P. A secured and intelligent communication scheme for IIoT-enabled pervasive edge computing. *IEEE Transactions on Industrial Informatics* **2020**, *17(7)*, 5128-5137.
169. Lawal, M. A.; Shaikh, R. A.; Hassan, S. R. An anomaly mitigation framework for iot using fog computing. *Electronics* **2020**, *9(10)*, 1565.
170. Alharbi, A.; Alosaimi, W.; Alyami, H.; Rauf, H. T.; Damaševičius, R. Botnet attack detection using local global best bat algorithm for industrial internet of things. *Electronics* **2021**, *10(11)*, 1341.
171. Nguyen, T. N.; Ngo, Q. D.; Nguyen, H. T.; Nguyen, G. L. An advanced computing approach for IoT-botnet detection in industrial Internet of Things. *IEEE Transactions on Industrial Informatics* **2022**, *18(11)*, 8298-8306.
172. Alqahtani, M.; Mathkour, H.; Ben Ismail, M. M. IoT botnet attack detection based on optimized extreme gradient boosting and feature selection. *Sensors* **2020**, *20(21)*, 6336.
173. Arshad, J.; Abdellatif, M. M.; Khan, M. M.; Azad, M. A. (2018, April). A novel framework for collaborative intrusion detection for m2m networks. In 2018 9th international conference on information and communication systems (ICICS) (pp. 12-17). IEEE.
174. Arshad, J.; Azad, M. A.; Abdeltaif, M. M.; Salah, K. An intrusion detection framework for energy constrained IoT devices. *Mechanical Systems and Signal Processing* **2020**, *136*, 106436.

175. Zhang, Y.; Deng, R. H.; Zheng, D.; Li, J.; Wu, P.; Cao, J. Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial IoT. *IEEE Transactions on Industrial Informatics* **2019**, *15(9)*, 5099-5108.
176. Qi, S.; Lu, Y.; Wei, W.; Chen, X. Efficient data access control with fine-grained data protection in cloud-assisted IIoT. *IEEE Internet of Things Journal* **2020**, *8(4)*, 2886-2899.
177. Tajalli, S. Z.; Mardaneh, M.; Taherian-Fard, E.; Izadian, A.; Kavousi-Fard, A.; Dabbaghjamanesh, M.; Niknam, T. DoS-resilient distributed optimal scheduling in a fog supporting IIoT-based smart microgrid. *IEEE Transactions on Industry Applications* **2020**, *56(3)*, 2968-2977.
178. Liu, J., Yuan, C., Lai, Y., & Qin, H. (2020). Protection of sensitive data in industrial Internet based on three-layer local/fog/cloud storage. Security and Communication Networks, 2020, 1-16.
179. He, S.; Cheng, B.; Wang, H.; Xiao, X.; Cao, Y.; Chen, J. (2018, April). Data security storage model for fog computing in large-scale IoT application. In IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 39-44). IEEE.
180. Ming, Y.; Yu, X. Efficient privacy-preserving data sharing for fog-assisted vehicular sensor networks. *Sensors* **2020**, *20(2)*, 514.
181. Xue, K.; Hong, J.; Ma, Y.; Wei, D. S.; Hong, P.; Yu, N. Fog-aided verifiable privacy preserving access control for latency-sensitive data sharing in vehicular cloud computing. *IEEE Network* **2018**, *32(3)*, 7-13.
182. Fan, K.; Wang, J.; Wang, X.; Li, H.; Yang, Y. Secure, efficient and revocable data sharing scheme for vehicular fogs. *Peer-to-Peer Networking and Applications* **2018**, *11*, 766-777.
183. Adil, M.; Almaiah, M. A.; Omar Alsayed, A.; Almomani, O. An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks. *Sensors* **2020**, *20(8)*, 2311.
184. Bany Salameh, H.; Derbas, R.; Aloqaily, M.; Boukerche, A. (2019, November). Secure routing in multi-hop iot-based cognitive radio networks under jamming attacks. In Proceedings of the 22nd International ACM Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (pp. 323-327).
185. Abhishek, N. V.; Gurusamy, M. Jade: Low power jamming detection using machine learning in vehicular networks. *IEEE Wireless Communications Letters* **2021**, *10(10)*, 2210-2214.
186. Dovom, E. M.; Azmoodeh, A.; Dehghantanha, A.; Newton, D. E.; Parizi, R. M.; Karimipour, H. Fuzzy pattern tree for edge malware detection and categorization in IoT. *Journal of Systems Architecture* **2019**, *97*, 1-7.
187. Guizani, N.; Ghafoor, A. A network function virtualization system for detecting malware in large IoT based networks. *IEEE Journal on Selected Areas in Communications* **2020**, *38(6)*, 1218-1228.
188. Khoda, M. E.; Kamruzzaman, J.; Gondal, I.; Imam, T.; Rahman, A. Malware detection in edge devices with fuzzy oversampling and dynamic class weighting. *Applied Soft Computing* **2021**, *112*, 107783.
189. Arp, D.; Spreitzenbarth, M.; Hubner, M.; Gascon, H.; Rieck, K.; Siemens, C. E. R. T. (2014, February). Drebin: Effective and explainable detection of android malware in your pocket. In Ndss (Vol. 14, pp. 23-26).
190. Allix, K.; Bissyandé, T. F.; Klein, J.; Le Traon, Y. (2016, May). Androzoo: Collecting millions of android apps for the research community. In Proceedings of the 13th international conference on mining software repositories (pp. 468-471).
191. Alaeiyan, M.; Dehghantanha, A.; Dargahi, T.; Conti, M.; Parsa, S. A multilabel fuzzy relevance clustering system for malware attack attribution in the edge layer of cyber-physical networks. *ACM Transactions on Cyber-Physical Systems* **2020**, *4(3)*, 1-22.
192. Shen, S.; Huang, L.; Zhou, H.; Yu, S.; Fan, E.; Cao, Q. Multistage signaling game-based optimal detection strategies for suppressing malware diffusion in fog-cloud-based IoT networks. *IEEE Internet of Things Journal* **2018**, *5(2)*, 1043-1054.
193. Alhawi, O. M.; Baldwin, J.; Dehghantanha, A. Leveraging machine learning techniques for windows ransomware network traffic detection. *Cyber threat intelligence* **2018**, 93-106.
194. Azmoodeh, A.; Dehghantanha, A.; Conti, M.; Choo, K. K. R. Detecting crypto-ransomware in IoT networks based on energy consumption footprint. *Journal of Ambient Intelligence and Humanized Computing* **2018**, *9*, 1141-1152.
195. Almashhadani, A. O.; Kaiiali, M.; Sezer, S.; O'Kane, P. A multi-classifier network-based crypto ransomware detection system: A case study of locky ransomware. *IEEE Access* **2019**, *7*, 47053-47067.
196. Maiorca, D.; Mercaldo, F.; Giacinto, G.; Visaggio, C. A.; Martinelli, F. (2017, April). R-PackDroid: API package-based characterization and detection of mobile ransomware. In Proceedings of the symposium on applied computing (pp. 1718-1723).

197. Sgandurra, D.; Muñoz-González, L.; Mohsen, R.; Lupu, E. C. Automated dynamic analysis of ransomware: Benefits, limitations and use for detection. *arXiv preprint* **2016** arXiv:1609.03020.
198. Tseng, A.; Chen, Y.; Kao, Y.; Lin, T. (2016). Deep learning for ransomware detection. IEICE Technical Report; IEICE Tech. Rep., 116(282), 87-92.
199. Ogundokun, R. O.; Awotunde, J. B.; Misra, S.; Abikoye, O. C.; Folarin, O. (2021). Application of machine learning for ransomware detection in IoT devices. In Artificial intelligence for cyber security: methods, issues and possible horizons or opportunities (pp. 393-420). Cham: Springer International Publishing.
200. Al-Hawawreh, M.; Den Hartog, F.; Sitnikova, E. Targeted ransomware: A new cyber threat to edge system of brownfield industrial Internet of Things. *IEEE Internet of Things Journal* **2019**, *6(4)*, 7137-7151.
201. Mukherjee, M.; Matam, R.; Shu, L.; Maglaras, L.; Ferrag, M. A.; Choudhury, N.; Kumar, V. Security and privacy in fog computing: Challenges. *IEEE Access* **2017**, *5*, 19293-19304.
202. Jbair, M.; Ahmad, B.; Mus' ab H, A.; Harrison, R. (2018). Industrial cyber physical systems: A survey for control-engineering tools. 2018 IEEE Industrial Cyber-Physical Systems (ICPS), 270-276.
203. Frey, M.; Gündoğan, C.; Kietzmann, P.; Lenders, M.; Petersen, H.; Schmidt, T. C.; ... Wählisch, M. (2019, April). Security for the industrial IoT: The case for information-centric networking. In 2019 IEEE 5th World Forum on Internet of Things (WF-IoT) (pp. 424-429). IEEE.
204. Fu, J. S.; Liu, Y.; Chao, H. C.; Bhargava, B. K.; Zhang, Z. J. Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing. *IEEE Transactions on Industrial Informatics* **2018**, *14(10)*, 4519-4528.
205. Xu, P.; He, S.; Wang, W.; Susilo, W.; Jin, H. Lightweight searchable public-key encryption for cloud-assisted wireless sensor networks. *IEEE Transactions on Industrial Informatics* **2017**, *14(8)*, 3712-3723.
206. Schütte, J.; Brost, G. S. (2018, August). LUCON: Data flow control for message-based IoT systems. In 2018 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE) (pp. 289-299). IEEE.
207. Moustafa, N.; Adi, E.; Turnbull, B.; Hu, J. A new threat intelligence scheme for safeguarding industry 4.0 systems. *IEEE Access* **2018**, *6*, 32910-32924.
208. De Donno, M.; Felipe, J. M. D.; Dragoni, N. (2019, June). ANTIBIOTIC 2.0: A fog-based anti-malware for Internet of Things. In 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 11-20). IEEE.
209. De Donno, M.; Dragoni, N. (2019, May). Combining AntibIoTic with fog computing: AntibIoTic 2.0. In 2019 IEEE 3rd International Conference on Fog and Edge Computing (ICFEC) (pp. 1-6). IEEE.
210. De Donno, M.; Dragoni, N.; Giaretta, A.; Mazzara, M. (2018). AntibIoTic: protecting IoT devices against DDoS attacks. In Proceedings of 5th International Conference in Software Engineering for Defence Applications: SEDA 2016 5 (pp. 59-72). Springer International Publishing.
211. Eldefrawy, M. H.; Pereira, N.; Gidlund, M. Key distribution protocol for industrial Internet of Things without implicit certificates. *IEEE Internet of Things Journal* **2018**, *6(1)*, 906-917.
212. Li, F.; Hong, J.; Omala, A. A. Efficient certificateless access control for industrial Internet of Things. *Future Generation Computer Systems* **2017**, 76, 285-292.
213. Cui, H.; Deng, R. H.; Liu, J. K.; Yi, X.; Li, Y. Server-aided attribute-based signature with revocation for resource-constrained industrial-internet-of-things devices. *IEEE Transactions on Industrial Informatics* **2018**, *14(8)*, 3724-3732.
214. Xiong, H.; Bao, Y.; Nie, X.; Asoor, Y. I. Server-aided attribute-based signature supporting expressive access structures for industrial internet of things. *IEEE Transactions on Industrial Informatics* **2019**, *16(2)*, 1013-1023.
215. Bao, Y.; Qiu, W.; Cheng, X. Efficient and fine-grained signature for IIoT with resistance to key exposure. *IEEE Internet of Things Journal* **2021**, *8(11)*, 9189-9205.
216. Basic, F.; Gaertner, M.; Steger, C. (2021, October). Towards trustworthy NFC-based sensor readout for battery packs in battery management systems. In 2021 IEEE International Conference on RFID Technology and Applications (RFID-TA) (pp. 285-288). IEEE.
217. Basic, F.; Laube, C. R.; Steger, C.; Kofler, R. (2022, May). A Novel Secure NFC-based Approach for BMS Monitoring and Diagnostic Readout. In 2022 IEEE International Conference on RFID (RFID) (pp. 23-28). IEEE.

218. Basic, F.; Gaertner, M.; Steger, C. Secure and Trustworthy NFC-Based Sensor Readout for Battery Packs in Battery Management Systems. *IEEE Journal of Radio Frequency Identification* **2022**, *6*, 637-648.
219. Sharma, G.; Kalra, S. A lightweight multi-factor secure smart card based remote user authentication scheme for cloud-IoT applications. *Journal of information security and applications* **2018**, *42*, 95-106.
220. Bae, W. I.; Kwak, J. Smart card-based secure authentication protocol in multi-server IoT environment. *Multimedia Tools and Applications* **2020**, *79*, 15793-15811.
221. Zhou, S.; Gan, Q.; Wang, X. Authentication scheme based on smart card in multi-server environment. *Wireless Networks* **2020**, *26*, 855-863.
222. Liang, W.; Xie, S.; Zhang, D.; Li, X.; Li, K. C. A mutual security authentication method for RFID-PUF circuit based on deep learning. *ACM Transactions on Internet Technology (TOIT)* **2021**, *22(2)*, 1-20.
223. Aghili, S. F.; Mala, H.; Kaliyar, P.; Conti, M. SecLAP: Secure and lightweight RFID authentication protocol for Medical IoT. *Future Generation Computer Systems* **2019**, *101*, 621-634.
224. Tewari, A.; Gupta, B. B. Secure timestamp-based mutual authentication protocol for IoT devices using RFID tags. *International Journal on Semantic Web and Information Systems (IJSWIS)* **2020**, *16(3)*, 20-34.
225. Izza, S.; Benssalah, M.; Drouiche, K. An enhanced scalable and secure RFID authentication protocol for WBAN within an IoT environment. *Journal of Information Security and Applications* **2021**, *58*, 102705.
226. Gope, P.; Amin, R.; Islam, S. H.; Kumar, N.; Bhalla, V. K. Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment. *Future Generation Computer Systems* **2018**, *83*, 629-637.
227. Lipps, C.; Herbst, J.; Schotten, H. D. (2021, February). How to Dance Your Passwords: A Biometric MFA-Scheme for Identification and Authentication of Individuals in IIoT Environments. In ICCWS 2021 16th International Conference on Cyber Warfare and Security (p. 168). Academic Conferences Limited.
228. Zhao, G.; Zhang, P.; Shen, Y.; Jiang, X. Passive user authentication utilizing behavioral biometrics for IIoT systems. *IEEE Internet of Things Journal* **2021**, *9(14)*, 12783-12798.
229. Sarier, N. D. Efficient biometric-based identity management on the Blockchain for smart industrial applications. *Pervasive and Mobile Computing 2021*, *71*, 101322.
230. Jayasinghe, U.; Lee, G. M.; MacDermott, Á.; Rhee, W. S. TrustChain: A privacy preserving blockchain with edge computing. *Wireless Communications and Mobile Computing* **2019**, *2019*.
231. Huang, B.; Cheng, X.; Cao, Y.; Zhang, L. (2018, October). Lightweight hardware based secure authentication scheme for fog computing. In 2018 IEEE/ACM Symposium on Edge Computing (SEC) (pp. 433-439). IEEE.