INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE
A. Karakaya et al., Vol.10, No.4, pp.138-152

A Survey on Security Requirements, Threats and Protocols in Industrial Internet of Things

Aykut Karakaya[1], Ferhat Arat[2]

[1]Department of Computer Technologies, Bulent Ecevit University, Zonguldak, TURKEY
[2]Department of Software Engineering, Samsun University, Samsun, TURKEY
Corresponding Author: aykut.karakaya@bil.omu.edu.tr

Review Paper Received: 03.12.2021 Revised: 18.12.2021 Accepted: 19.12.2021

Abstract—With the tremendous success and prevalence of the Internet of Things (IoT) consumer technologies are shifted to distinct areas. Therefore, the IoT paradigm is evoluting with people interactions by devices and applications. The Industrial Internet of Things (IIoT) is an form of this recent evolution. IIoT is emerged considering various components of industrial requirements such as automation, monitoring, management. Depending on aims such as large scalability, high cost minimization on manufacturing, safety and management, the IIoT technology provides many benefits. While huge scope and many advantages of this intelligent decision and analysis paradigm which termed as IIoT, it also hosts serious security issues such as threats and vulnerabilities. Although, many similarities with IoT security challenges such as lack of standardization and device characteristics, when considering scope of IIoT, security must tackle in different aspects. In this article, we examine the IIoT concept in terms of manufacturing domain. We investigate the relationship between IIoT and IoT and highlighted their differences at manufacturer/consumer point. We present a comprehensive security study on IIoT technology. We define the IIoT technology on security direction. We also summarize studies on literature over the period 2017-2022 on IIoT security, focusing in particular on the security challenges, attacks and issues. We presents security, threats, challenges and issues of IIoT systems considering all levels. Finally, we highlight IIoT protocols in terms of security aspect and we emphasize open problems.

Keywords—IIoT, Security, Threats, Protocols.

1. Introduction

The Internet of Things (IoT) generates a concept including various type of interconnected devices. These devices which are form of heterogeneous network technology are ranging from small sensors to complex controllers and home appliances. IoT technology, which plays the role of facilitating daily life at the consumer level, is widely used in different fields. With technological developments and increasing demand, hardware and software costs are decreasing. Decreasing of these costs create motivation for the use of IoT devices apart from simple smart applications. Initially considered on consumer dimension, IoT technology and depending applications are used in a several of formats and sectors in a customized way, depending on the success and prevalence of use. One of these sectors is the Industry. It is commonly referred to as Industry 4.0, i.e., the fourth industrial revolution, or as industrial Internet of Things (IIoT) [29]. IIoT is a technology which allows to system monitoring, data exchange and smart decision. With this

technology concept, flexibility and dynamism are increased at the manufacturer level, advantages such as process optimizations, maintenance, production and distribution ease are provided. As in IoT systems, the main output is feedback mechanism in IIoT systems. In the IIoT structure, after the large amount of sensed and collected data are transmitted to the processing point over the internet, feedback is made in the production and optimization dimension with the decision-making mechanism. Unlike the traditional cellular technologies such as 4G/5G and others, IIoT technologies purpose low energy consumption, limited hardware requirements and low cost. However, as in the other Internet technologies, security, privacy and reliability are significant features and desired requirements in IIoT.

The security of IIoT must be characterized as distinctive perspective. Since, serious safety and/or economic loss implications are quite different than IoT technology. In IoT nature, security and privacy attacks target consumer yet, a similar attack on IIoT network can cause huge effects over the manufacturing. In this respect, IIoT requires a higher grade security mechanism that takes into account requirements, nature of devices in the network, recovery mechanism in the event of an attack, and similar factors [30]. Therefore, security and privacy in IIoT systems are investigated by various perspective in the literature. In [31], low latency, high service performance and effective bandwidth aware architecture is proposed for IIoT systems. The proposed structure works based on fog computing which considering context of IIoT. [32], Hussain et al. proposed an model to provide device configuration and management during setup session. The proposed model works based on deep learning approach and aims to solve resource management problem considering security issue. In order to prevent malicious software injecting, a deep learning method is proposed by Ullah et al. [33]. The proposed method considers privacy and works based on deep learning methods. In [34], personalized privacy protection framework is proposed based on game theory and data encryption for IIoT systems. The proposed model aims to ensure data confidentiality, integrity, and real-timeness.

1.1. Motivation and Research Method

When considering the usage area, scope and the advantages of IIoT systems, security is an open problem in the literature. Numerous security studies are exist in IoT and IIoT domains. In this paper, the current state of the art of IIoT concept is presented. Next, the IIoT structure is summarized in terms of architecture and its differences from the traditional IoT concept. We focus on analyzing of IIoT system and security issues. Therefore, security risks, challenges and attacks are presented in the IIoT. The main contributions of this article is listed as belows:

- We emphasize the IIoT structure in terms of architectural design and we investigate IIoT applications considering IoT technologies.
- We describe the IIoT concept on manufacturing perspective with real time applications.
- We present the security threats and challenges on IIoT considering all layers and focusing usage domain.
- We summarize the IIoT layer protocols depending on security challenges and issues.

Security is the main focus of this study. Studies on IIoT security in the literature are examined by using "IIoT AND (Security OR Threats OR Applications)" keywords while generating all sections. We considered the real time examples of

IIoT systems and security approaches while investigating the literature. In addition, we prepared a review of the literature over the period 2017-2022 on IIoT security, focusing in particular on the security challenges, attacks and issues of the IIoT. As a difference from other existing surveys, we present general overview of all security threats and issues considering layers, protocols and applications. We also tackle IIoT concept in terms of operational technologies, manufacturing and real-time usages. The number of papers which are examined according to our study in "IIoT AND security" search in the databases is shown in Table 1. Although there are more studies in the considered databases than listed in the table, only studies which are proper with our motivation are shown numerically. According to investigated studies in the databases, the journals with the highest number of papers in these search results are IEEE Transactions on Industrial Informatics (31) for IEEExplore, Procedia Manufacturing (42) for Science Direct, Sensors (16) for MDPI.

TABLE 1: Number of papers in "IIoT AND security" search in databases

Databases	2017	2018	2019	2020	2021	2022
IEEExplore	-	8	14	23	30	3
Science Direct	-	16	19	25	46	3
MDPI	1	6	9	17	22	-
Web of Science	7	23	36	45	52	2
Scopus	6	18	22	34	48	6
Dergipark	-	-	-	-	1	-

The number of papers which are examined according to our study in "IIoT AND Threats" search in the databases is shown in Table 2. Although there are more studies in the considered databases than listed in the table, only studies which are proper with our motivation are shown numerically. According to the databases, the journals with the highest number of papers in these search results are IEEE Transactions on Industrial Informatics (13) for IEEExplore, Journal of Network and Computer Applications (16) for Science Direct, Sensors (9) for MDPI.

TABLE 2: Number of papers in "IIoT AND threats" search in databases

Databases	2017	2018	2019	2020	2021	2022
IEEExplore	1	3	8	16	9	2
Science Direct	3	12	29	38	52	16
MDPI	-	4	7	17	23	-
Web of Science	2	14	25	28	34	1
Scopus	3	15	32	61	65	2
Dergipark	-	1	-	-	-	-

The number of papers which are examined according to our study in "IIoT AND applications" search in the databases is shown in Table 3. Although there are more studies in the considered databases than listed in the table, only studies which are proper with our motivation are shown numerically. According to the databases, the journals with the highest number of papers in these search results are IEEE Transactions on Industrial Informatics (56) for IEEExplore, Procedia Manufacturing (52) for Science Direct, Sensors (28) for MDPI.

TABLE 3: Number of papers in "IIoT AND applications" search in databases

Databases	2017	2018	2019	2020	2021	2022
IEEExplore	6	30	48	46	59	4
Science Direct	13	22	39	28	62	16
MDPI	3	14	17	26	33	-
Web of Science	14	24	45	58	56	4
Scopus	12	30	52	48	66	21
Dergipark	-	1	-	2	-	-

Web of Science and Scopus generally contain papers that have been founded in other databases. There are very limited papers in Dergipark.

1.2. Organization

The remainder of this study is structured as follows. Section 2 presents IIoT structure considering available literature studies. Section 3 describes differences between IIoT and consumer IoT, also gives real application instances of IIoT systems. Then, in Section 4, the security threats, challenges, vulnerabilities and issues on IIoT are emphasized. Section 5 highlights list of open research challenges and open problems.

2. IIoT Architecture

The Industrial Internet of Things include traditional Industrial Control Systems (ICS) and Operational Technology (OT) [35]. IIoT systems support several significant sectors and infrastructures with these technologies. As in the available network systems and technologies, IIoT technology has architecture to interoperate with mentioned technologies. Each architecture is a high level abstractions which defines various protocols, application scenarios, issues and challenges. Designed and proposed IIoT architectures need to highlight extensibility, scalability, modularity, and interoperability among heterogeneous devices and applications using different technologies [36]. Different requirements have emerged depending on the scope of IoT technologies, their application areas and the increase in the number of users. Accordingly, different protocols, services and applications are designed for smart device technology IoT and its customized form which is termed as IIoT networks.

The designed protocol and services work on different layer in IIoT architecture to provide user and manufacturer requirements. In this context, various architecture models are proposed to identify layer based tasks of IIoT protocol

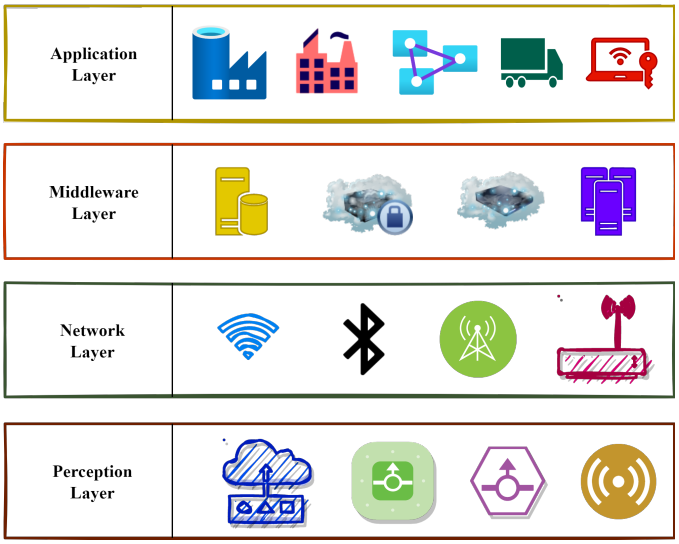

Fig. 1: Multi-tier structure of IIoT

and services. Generally, the designed models have multi-tier structure [41]. For instance, in [37] and [38], three layer basic architecture is proposed which has perception, network and service layers. By Industrial Internet Consortium (IIC), the reference architecture is defined considering technical and security requirements. According the designed architecture, each tier divided into sub-tiers. The generated layers are named as edge, platform and enterprise [40], [39]. Industrial Automation and Control Systems (IACS) is standartized IIoT scheme by multi-layered structure. This architecture consists of multiple zones and there are five level. Fig. 1 shows an instance of IIoT multi-tier architecture.

3. From IoT to IIoT

The IIoT defines usage of sensors, actuators and management systems in order to improve manufacturing and industrial processes. This technology is alsw known as Industrial Internet or Industry 4.0. Although, IoT and IIoT technologies have common and similar platform and devices, these two technologies are used for distinctive purposes

TABLE 4: Comparison Between Consumer IoT and Manufacturer IIoT

Manufacturer IIoT	Consumer IoT
Works large scale networks.	Related with small scale networks.
Focuses on industrial domains by application, service and devices	Focuses on general usage area such as individual usage, smart objects.
Requires not only Wi-Fi connection but also cellular connection type.	Requires Wi-Fi connection and configuration to transmit data.
Device and services have long life period.	Device and services have short life period.
Designed for manufacturing areas to provide resource efficiency and management.	Designed for consumer areas by applications and services.
Requires higher bandwidth generally.	High bandwidth is not necessary.
Used in industrial and professional service domains.	Covers covers a wide range of industries and users.
Require high levels of precision and accuracy to provide efficiency and reliability.	Quality is not depending on directly precision and accuarcy.
Energy harvesting is a promising approach.	Not guarantee energy and resource efficiency.
Focuses on data processing and decision making.	Focuses on data collection and transmission.

and methods by consumer and manufacturers. Table 4 shows comparison between manufacturer IIoT and IoT concepts. Basically, IoT and depending applications provides ease of usage to consumers in different application domains such as agriculture, healthcare, healthcare. IoT devices and services are designed for works small scale networks and they have short life cycle in terms of device characteristics. IIoT applications connect machines and devices in various manufacturing areas. The applications and services which have long life cycle, and work large scale networks are characterized by a strong interconnection between controllers, monitors and devices. In IIoT concept, devices are not directly connected to Internet or cloud systems. IIoT services purposes manufacturing optimization and management. In other words, IIoT applications are directly concerned with improving efficiency, management and monitoring.

3.1. IIoT in Real-Time Domains

The IIoT provides several benefits from consumer to manufacturer. Especially, in manufacturing perspective, organizations can use real-time application and services by processing generated data. By this way, more efficient manufacturing and maintenance conditions are emerged and operational and management efficiency can be achieved. Using real-time data for manufacturing provides different advantages to manufacturers. The IIoT works beyond simple sensing and transmission attributes. This technology also allows to more informed decisions and this intelligent decision is one of main purpose of IIoT sytems as production and maintenance tasks. In addition, IIoT also allows to customization according to customer requirements. Thus, manufacturers build more customer-aware roadmaps. Fig. 2 highlights IIoT and IoT concepts.

With ease of usage and advantages, IIoT technologies take place in real-time areas. For instance, Airbus Company which is known as jetliner producer, integrated sensor and chips into machines in order to reduce manufacturing errors by using wearable technologies. Therefore, manufacturing and employees safety is provided. In another instance of IoT technologies is robotic developments on manufacturing areas in the

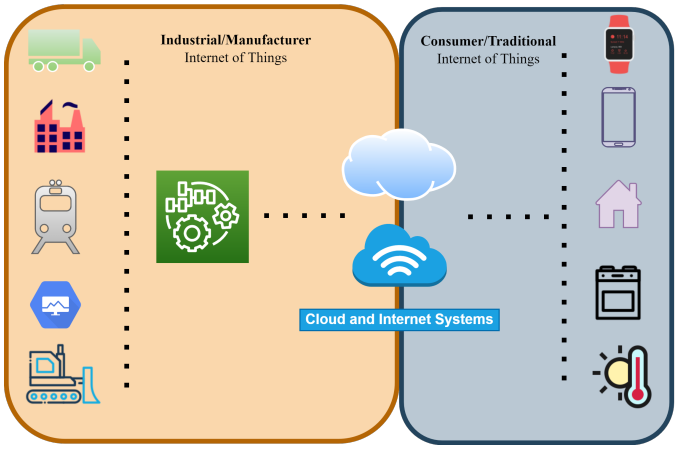

Fig. 2: IIoT and IoT concept

robotic manufacturer Fanuc Company. By using the high capability sensors on robotics with cloud based data methods, failure prediction and cost reduction is provided [42]. The Tesla Company, which is one of the best known in electric vehicle manufacturing, uses IIoT technologies in order to improve efficiency and to produce user friendly vehicles which have ability to control and check from anywhere. By Magna Steyr which is an Austrian automotive manufacturer, smart packing and tracking technologies are using with Bluetooth network in order to provide time and employee efficiency.

There are application examples in IIoT such as smart factory, smart grid, smart production, health systems. With sensor nodes placed on monitored objects, data is collected and transmitted to a data center and there is processed. While the results obtained trigger an another machine in autonomous systems, information is transferred to the monitoring user in other systems. These applications provide combine mobile IoT supported dynamic nodes to monitor traffic flows, service to many devices with self-configuration capacity, and provide information management, data flow support in a wide range of networks [43]. In addition, these applications require real-time and secure transactions. For this reason, high-speed data transmission environment, low-latency processing of data, energy savings and, lightweight protocols that provide low latency should be provided.

4. Security Threats, Challenges, Issues

In the security of IoT systems, it is necessary to consider the security of each device and module because the attack on an IoT system is not only limited to the attacked device, but also it can manipulate the entire IoT infrastructure. In addition to the known attack types, there are also attack types specific to IoT systems. Attacks are generally aimed at stealing information, slowing down or stopping the service, damaging reputation, and damaging the system. For these reasons, data centers are the most important element that must be secure. Data centers in industrial IoT (IIoT) systems are designed using paradigms such as cloud computing and fog computing. Because fog computing provides a local solution at the edge of the network, it has higher performance than cloud computing [1]. It is therefore suitable for structures operating in limited coverage, similar to IIoT systems. Attacks on cloud/fog based data centers, attacks on edge devices and general attacks organized for industrial IoT are examined.

In addition, with the effect of 5G technology, high-speed communication is aimed in Industry 4.0 operational technology networks. However, as in almost every development, 5G technology brings with it a number of security problems.

In this section, studies focusing on security requirements and attack types for IIoT systems are reviewed. The concept of IIoT covers a very wide field of work. Production facility, industry,

factory, logistics, smart city are some of them. The attack scenarios that each cyber-physical or IIoT system may be exposed to may be similar, or they may differ in specific areas of use. For example, in a production facility, since the machines are close to each other, a system can be designed with local solutions using fog computing by limiting the coverage area. However, when a logistics company is considered, autonomous machines in the company may need to contact carrier vehicles and the system can be designed using remote cloud computing. Thus, similar attacks can be carried out in different ways or completely different types of attacks can be used between these two IIoT systems. In fog computing systems, storage, computing and network resources are controlled locally by a user, while in cloud computing systems they are controlled by the cloud provider [2]. Therefore, the cloud provider must also be secure.

Although the purpose of developing IIoT architectures seems to be performance, functionality and fast communication, the security phase is of crucial importance as in every system. In this context, in addition to the basic principles of security known as confidentiality, integrity and availability, principles such as authentication, access control, sustainability, flexibility, and data freshness must also be handled for IIoT systems. Based on industrial areas, the order of importance of the basic principles is stated as availability, integrity and confidentiality [3]. There are many security solution approaches in the literature that provide the basic principles for IIoT.

The security and privacy requirements for IIoT applications can be listed as follows [4], [5]:

- Authentication: Resource constrained IoT devices cannot perform encryption operations required for authentication. For this, high-cost storage and data processing needs are provided by external sources such as fog/cloud. Users and system elements have to verify their identities in the fog/cloud network in order to receive uninterrupted service. Access by unauthorized users is blocked.
- Data Protection: In IoT applications, large amounts of data can be generated depending on the number of devices. The processing and storage of this data is done in fog/cloud nodes. Since it is costly to determine the accuracy of data by resource-constrained IoT devices, this need is met by data centers such as fog/cloud computing.
- Confidentiality: Data must be kept confidential during transmission from IoT node to fog node or from fog node to cloud. When an IoT edge device needs information processing and storage, it communicates with the fog/cloud node.Since the end nodes are resource constrained, lightweight encryption structures are used to secure this communication.
- Malicious User and Intrusion: A malicious node in the IoT environment causes data to be mistranslated, modified, or stolen. When the devices on the network cannot mutually authenticate each other, the attacker node can initiate a DoS (Denial of Service) attack by continuously sending a storage or data processing request to the fog/cloud node. Nodes access is limited to protect from malicious node.
- Data Integrity: Data corruption caused by attacks that may occur in IoT systems must be detected by the system. Deterioration of data integrity can cause machines in a facility to malfunction and produce inaccurate data.
- Availability: Users must be protected from attacks aimed at preventing uninterrupted service from system resources. Denial of Ser-

vice (DoS) and Distributed Denial of Service (DDoS) are some of the attacks that affect availability.

- Heterogeneity: Data must be transmitted to the fog/cloud center from a large number of devices with different characteristics. However, computing power and cost increase when different communication needs are met. Devices in IIoT systems can communicate wirelessly because they generally support 802.15.x protocols.
- Computing Cost: In IoT applications, the computational power of fog/cloud systems is needed to reduce latency. Processes such as processing and storing data, generating real-time response, detecting attacks are difficult to do on resource-constrained devices.
- Conscious User: Users may not be aware of the security risks that may occur when using IIoT technologies. [6]. If a user is attacked and this attack is successful, the entire network can be affected. For this reason, the important assets of the system should not be open to the initiative of standard users and a security policy should be adopted that raises users' awareness of security risks.

4.1. Security Threats of IIoT Systems

IIoT systems are vulnerable to attacks in terms of many parameters such as communication, connectivity, infrastructure. IIoT infrastructure requires effective defense against cyber threats to mitigate the impact of vulnerability [7]. The types of attacks against IIoT are inherently similar to attacks against standard IoT. But when an attack is successful, there is a difference in the severity of the results of the attack. For example, an attacker's penetration into the IoT network can cause damage, such as a privacy breach or data theft, while a similar attack on an IIoT can cause a major disaster, such as network downtime, network congestion, production or business process stoppage. Therefore, IIoT systems require a higher level of security infrastructure that takes into account the accuracy of data, the topology of the network, the structure of devices on the network, the recovery mechanism in the event of an attack, and similar factors [8].

Malware: The most important threat in mobile IIoT networks is malware that causes theft or manipulation of IoT data, user identities, personal and corporate information. A malware installed on a mobile device can lead to personal data leakage, loss of reputation that damages social image, service problems that disrupt the organization of businesses, and financial loss [9].

Internal attacks: It is a type of attack that makes the working environment worse and more unsafe [10]. It is a significant threat to sensor-cloud/fog services in a system [11]. For IIoT systems, it can lead to resource abuse, false feedback, machine misdirection, and faulty production. In addition, malicious cloud/fog service providers can also lead to internal data leaks. Therefore, companies providing these services should be reliable and ensure security requirements. Security requirements such as access control and authentication should be supported to prevent unauthorized users from accessing the system. An attacker who is included in the network can trigger internal attacks such as DoS, MITM, privilege escalation.

DoS and DDoS attacks: These attacks are one of the popular attack types in almost every technology, from traditional network structures to the widely used IoT network structures in recent years. It is also the most common type of attack for IIoT systems [27]. Although there

are differences in the implementation and activation of attacks in terms of the infrastructure technology used by the victim, the main purpose is to overflow the buffers, slow down and prevent the communication of the system. In this way, the attacker can activate other dangerous attacks to capture data. DoS attacks pose a serious threat as IIoT edge devices are low-power, low-capacity. Networks without authentication and intrusion detection mechanisms have no resistance to these attacks. In networks with a strong authentication and intrusion detection mechanism, attackers must capture a legitimate device and impersonate that device in order to carry out these attacks. The vulnerabilities of all devices, protocols and technologies used in the network infrastructure can be exploited for impersonation. For example, in a factory network where automatic stock, product and inventory tracking is carried out using RFID technology, the attacker can generate noise by sending radio frequency signals, and can prevent legitimate communication. The example is shown in Figure 2. 3. The method may be different, but a similar effect can be achieved on systems using other technologies or protocols. DDos attack is a coordinated attack of many distributed devices that are compromised and used as bots [28]. The attacker sends a large number of protocol packets to the network, increasing the traffic of the network and causing buffer overflows of the devices in the network infrastructure. These overflows prevent a legitimate communication. TCP SYN flood, UDP flood, ARP flood, MAC flood are some of them. In order for the attacker to perform a DDoS attack, he/she must capture a large number of objects in the network and create an organized data traffic. Besides DoS and DDoS, there is persistent DoS attack, where an attacker damages a legitimate device either physically or by installing a corrupted BIOS with malware [28]. These attacks can be carried out to disable critical units such as electrical transformer, water treatment plant, gas discharge system.

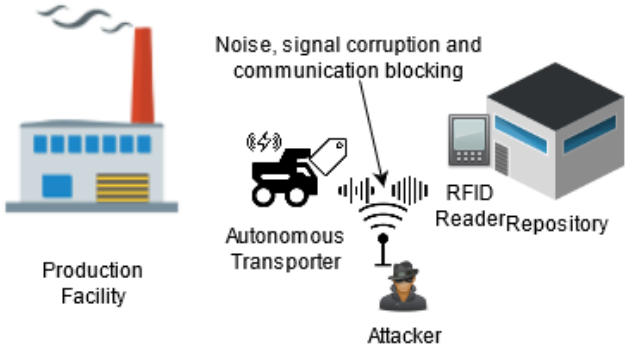

Fig. 3: An example of DoS for IIoT (using RFID)

Physical attacks on devices: For the successful operation of IIoT applications, the devices must be correctly positioned and the devices and communication must be secure. IIoT and Industry 4.0 generally aim to enable smart devices to communicate with each other and carry out activities such as production, logistics, failure control and feedback. For this reason, manipulations that may occur in the communication of smart devices may adversely affect the primary operation output for IIoT systems. Theft of devices, deletion or alteration of data by starting MITM, activating DoS or DDoS attacks, launching different attacks using the identity of the compromised devices are among the most important attack methods. Therefore, the security of the devices is extremely important. However, in IIoT systems, the security of the environment in which they are located is prioritized rather than the physical security of the end devices. This makes devices vulnerable to physical attacks such as invasive hardware attacks, side-channel attacks, and reverse engineering [13]. In addition, remote connection to the system can be provided so that devices can be

controlled, updated and booted. Devices may also have vulnerabilities against some other attacks, depending on the method used in the remote connection.

Hostile localization attack: Spectrum scarcity and security needs of cyber physical systems (CPS) are major challenges for IIoT systems. Because industrial CPS captures critical data and transmits it wirelessly, IIoT systems are attractive to attackers [12]. This attack is a physical layer attack and aims to geo-locate edge devices. This poses a threat to the overall security of the IIoT system as well as this device. Based on the received signal strength (RSS) on mobile smart devices, the distances to the device are estimated by capturing the signal. And thus, the location of the device can be found with the trilateration technique, as in GPS systems. In this way, geographical locations of mobile devices on IIoT systems can be obtained and this mobile device can be manipulated. The geolocation process is shown in Fig. 4.

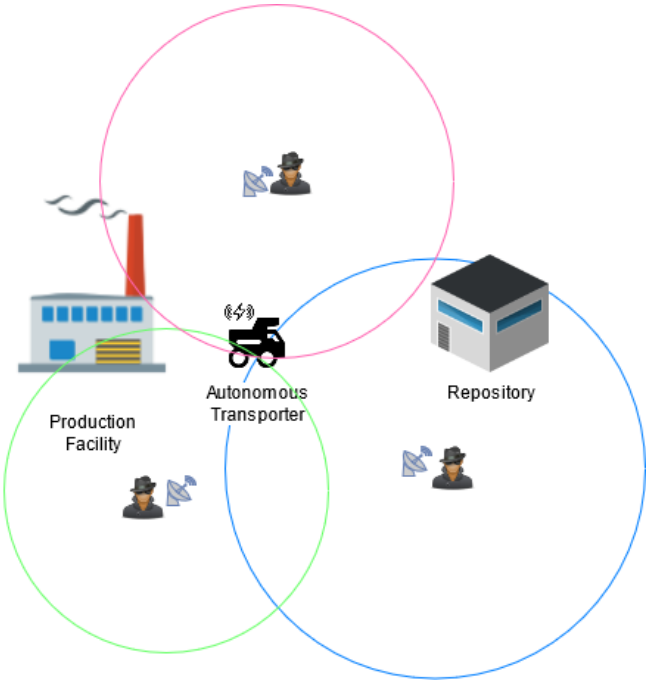

Fig. 4: The geolocation process

Cryptographic attacks: Certain cryptographic algorithms are used to provide security principles such as data confidentiality, authentication, and data integrity. Attacks such as brute force, frequency analysis, insecure certificate providers, key prediction with packet capture, and finding unique device identifiers can be carried out on encryption systems. These attacks allow many other attacks to activate. Any user can be seized and the entire network can be threatened and cause significant losses for the company. Device identifiers, device IDs, private key and symmetric key and similar cryptographic structures must be stored securely [13]. A suitable and strong encryption system and key size should be preferred to prevent malicious attacks.

MitM attacks: In this attack, the attacker listens, transmits, and modifies traffic between two endpoints [26]. It is carried out by poisoning the ARP in the local network. The attacker constantly sends an ARP response packet to the target node using the victim's IP address and his own MAC address, and by convincing the target, he poisons the target's ARP table with fake information. By applying a similar process to both ends, the attacker transfers the traffic between the two end systems. It is the second most popular attack type for IIoT systems [27]. An attacker who captures one of the IIoT end devices can initiate MITM on the internal network. Thus, the attacker can steal and manipulation information between nodes and even pave the way for other attacks.

Attacks on communication protocols: Communication protocols that determine the communication rules between devices can cause significant attacks in IIoT systems. An attacker using the vulnerabilities of the protocols can capture the

transmitted packets and parse these packets. Thus, by activating a MITM attack, the attacker can obtain important information and cause false data to be sent to the target by manipulating the protocol packets. The types of attacks against some IIoT protocols are as follows:

- The LoRaWAN protocol configures end nodes to transmit data over IP to the network server. This protocol is vulnerable to selective-jamming attacks. Having knowledge of the details of the system, an attacker selectively identifies high-importance packets and jams the traffic of the target end node [14].
- The 6LoWPAN is a protocol that describes low-power wireless personal area networks using IPv6. It is vulnerable to security threats from the local network and the internet. As it consists of a combination of IPv6 and WSN networks, situations that threaten both can also pose a threat to 6LowPAN [15]. This protocol is vulnerable to attacks such as unauthorized eavesdropping, DoS and Hello flood attacks that cause network congestion, misdirection of packets, Sybil attacks that cause impersonation of users, Sinkhole used to pull traffic to a specific node, and Wormhole which creates tunnels in the network with two malicious nodes. IIoT systems using 6LoWPAN have to use multiple additional security protocols.
- The ZigBee protocol, like any wireless communication, is vulnerable to many network and penetration attacks [16]. It uses the AES-128 encryption algorithm. Since ZigBee is effective in resource-constrained systems, it cannot use standard security structures like public key mechanisms. It can be expose to attacks such as DoS and flood attacks aimed at disconnecting, synchronization attacks that perform lost frame retransmission, Wormhole and misdirection attacks, eavesdropping and tampering.
- CoAP is a web transport protocol developed for resource constrained devices, a customized version of HTTP, capable of machine-to-machine communication for IIoT networks. [17]. The CoAP structure uses UDP as the transport protocol and DTLS as the security support. It can be exposed to attacks such as: Attack on complex protocol parsers, MITM, packet hijacking and DoS attack by increasing the size of packets, IP spoofing, attacks on encryption keys on low-power end devices, spoofing of messages [18].
- MQTT is a lightweight messaging and information exchange protocol based on subscriber-broadcast architecture [19]. MQTT security is provided by SSL/TLS. There is no verification mechanism as any user can become a publisher or subscriber. For this reason, many attacks can be launched, especially DoS and DDoS attacks. For example; An attacker can initiate a SlowITe attack, a type of DoS, by establishing multiple connections with the MQTT server using the lowest bandwidth [20]. It is vulnerable to packet capture and eavesdropping and manipulation attacks, as lost messages are difficult to sort and resend.
- XMPP is an instant messaging protocol that exchanges data for clients and servers [21]. XMPP uses Base64-based SASL, which hides passwords and provides authentication, and TLS, which protects the channel against stream eavesdropping and tampering. Since its structure is similar to SMTP, the addresses in the ”from” and ”to” fields are likely to be manipulated by attackers. During

transmission, some of the streams can proceed unprotected and thus different attacks can be activated. Attacks such as password capture, password guessing using dictionary attacks, retransmission, deletion and modification of XML structures in the data stream, privilege escalation, MITM and DoS can be performed.

- AMQP is a lightweight messaging protocol designed for reliability, security, and interoperability [22]. It supports both request-response and subscriber-broadcast mechanisms. It uses SASL and TLS/SSL structures for security. While transmitting data between two ends, it can be exposed to attacks such as MITM, DoS, session and identity-stealing replay, impersonation that makes the attacker pretend to be a legitimate user, tampering that aims to add, delete or modify data [23].
- DDS is a real-time, fast and high-performance protocol for interconnecting IoT devices [23]. DDS is used in many applications in important IIoT fields such as military, energy and aviation. Therefore, security issues are of much higher importance. Attacks such as MITM, which causes the monitoring, loss or alteration of message transmissions between devices, and DoS, which prevents legitimate communication by using malicious messages, can be initiated. In IIoT systems, attacks are difficult to detect, as system-specific methods such as Trending or Polling are often used instead of monitoring software [24].
- RPL is a distance vector algorithm based routing protocol for low power and lossy networks [25]. RPL has three security modes: unsafe mode with no security mechanism for control messages, preshared mode that secures control messages with symmetric keys assigned to devices before they are deployed, and authenticated mode that includes a key distributed by a certificate authority and allows new nodes to be added dynamically securely. Network topology, resources and traffic are targeted in attacks against RPL. There are attacks on topology such as wormhole, sinkhole, manipulation of the route table, attacks on resources such as flooding, routing table overflow, parent node modification, and attacks on traffic such as sniffing and traffic analysis [25]. The attacker node can exploit the vulnerabilities of the RPL protocol to penetrate legitimate nodes.

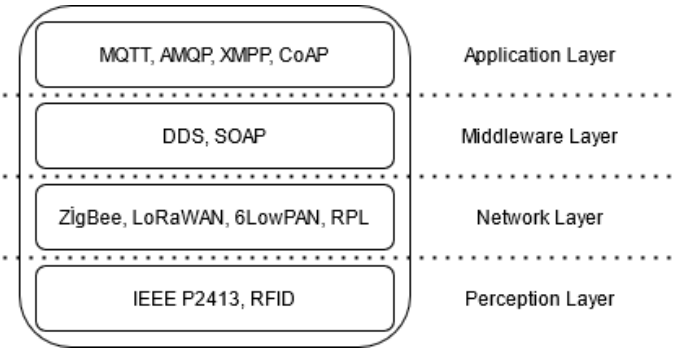

Fig. 5: IIoT protocols by layer

Table 5 shows comparison between manufacturer IIoT and IoT concepts in terms of security. Protocols in the traditional TCP/IP stack can be used in IIoT networks. These protocols also have some security vulnerabilities. However, in this section, protocols identified with IoT systems due to their low power and light weight are discussed. The exponential increase in the number of low-power devices in IIoT systems both complicates security issues and makes it inevitable to increase studies on this. The layers of these protocols in the stack defined for IIoT are shown in Figure 5.

TABLE 5: Comparison Between Consumer IoT and Manufacturer IIoT in terms of Security

Manufacturer IIoT	Consumer IoT
The damage probability depending on data manipulation can be higher.	The damage probability depending on data manipulation can be lower due to working area.
Works on local network.	Works on general network.
Can benefit from fog computing services to provide security.	Can benefit fog computing services due to application and determined storage method.
Due to low latency requirement, lighweight protocols is needed.	Low latency is not a priority as IIoT.
Depending on high volume data processing and transmission, data loss probablity is higher.	Due to limited data processing and transmission, data loss probablity is lower.
Since process-specific customized protocols can be developed in the Operational Technologies (OT), standard security solutions may be insufficient.	Known security solutions can be implemented due to uses the standard TCP/IP stack.
Uses protocols such as Modbus, Ethernet/IP, DNP3, and Profinet and these are rarely uses authentication, authorization or encryption methods.	Known authentication, authorization or encryption methods can be implemented due to usage of the standard protocols
Data backup is needed due to high data volume and provide data integrity.	Due to a relatively limited data volume, high storage spaces are not required.

5. Conclusions, Future Directions and Open Problems

Several technologies are emerged in recent years Internet of Things area. With the increasing of usage area and depending on user requirements. The Industrial Internet of Things concept is an relevant of IoT. With the customization and scalability perspective, IIoT is widespread for manufacturing and management systems. With the customization and scalability perspective, IIoT is widespread for manufacturing and management systems. These systems generate processed data and transmits over the Internet. In this process, data and systems become targets of attacks. Therefore security is significant research and development field. Depending on the complexity of the systems and devices, guaranteeing security in the IIoT is difficult. In this article, we analyzed IIoT paradigm in terms of security and privacy. We provided a systematic overview of IIoT by defining IIoT and its architecture. Some of open problems and research challenges on IIoT network are listed as below:

- Comprehensive security and privacy studies should investigate by considering different technologies and computing systems such as Deep Learning (DL) [44], fog computing [5]. .
- The risks of existing security attacks over IIoT layers and IIoT real-time applications should be highlighted.
- Considering high level complexity of IIoT devices, resource constrained security protocols are needed [41].

Acknowledgments

This paper is the extended version of [41] presented at ISCTurkey 2021. We thank Professor Sedat Akleylek for his valuable discussions.

References

[1] Bonomi, F., Milito, R., Zhu, J. & Addepalli, S. Fog Computing and Its Role in the Internet of Things.

Proceedings Of The First Edition Of The MCC. Workshop On Mobile Cloud Computing. pp. 13-16. https://doi.org/10.1145/2342509. 2342513, 2012.

[2] Chaudhary, D., Bhushan, K. Survey on DDoS attacks and defense mechanisms in cloud and fog computing. International Journal Of E-Services And Mobile Applications (IJESMA). 10, 61-83, 2018.

[3] 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. 22, 2489-2520, 2020.

[4] Mukherjee, M., Matam, R., Shu, L., Maglaras, L., Ferrag, M., Choudhury, N. & Kumar, V. Security and Privacy in Fog Computing: Challenges. IEEE Access. 5 pp. 19293-19304, 2017.

[5] Alrawais, A., Alhothaily, A., Hu, C. & Cheng, X. Fog computing for the internet of things: Security and privacy issues. IEEE Internet Computing. 21, 34-42, 2017.

[6] Bajramovic. Security Challenges and Best Practices for IIoT. INFORMATIK 2019: 50 Jahre Gesellschaft Für Informatik – Informatik Für Gesellschaft (Workshop-Beiträge). pp. 243-254, 2019.

[7] Tariq, U., Aseeri, A., Alkatheiri, M. & Zhuang, Y. Context-Aware Autonomous Security Assertion for Industrial IoT. IEEE Access. 8 pp. 191785-191794, 2020.

[8] Gebremichael, T., Ledwaba, L., Eldefrawy, M., Hancke, G., Pereira, N., Gidlund, M. & Akerberg, J. Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges. IEEE Access. 8 pp. 152351-152366, 2020.

[9] Sharmeen, S., Huda, S., Abawajy, J., Ismail, W. & Hassan, M. Malware Threats and Detection for Industrial Mobile-IoT Networks. IEEE Access. 6 pp. 15941-15957 (2018)

[10] Wang, T., Wang, P., Cai, S., Ma, Y., Liu, A. & Xie, M. A Unified Trustworthy Environment Establishment Based on Edge Computing in Industrial IoT. IEEE Transactions On Industrial Informatics. 16, 6083-6091, 2020.

[11] Wu, Y., Huang, H., Wu, Q., Liu, A. & Wang, T. A risk defense method based on microscopic state prediction with partial information observations in social networks. Journal Of Parallel And Distributed Computing. 131 pp. 189-199, 2019.

[12] Zhang, M., Chen, J., He, S., Yang, L., Gong, X. & Zhang, J. Privacy-Preserving Database Assisted Spectrum Access for Industrial Internet of Things: A Distributed Learning Approach. IEEE Transactions On Industrial Electronics. 67, 7094-7103, 2020.

[13] Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. & Ni, W. Anatomy of Threats to the Internet of Things. IEEE Communications Surveys Tutorials. 21, 1636-1675, 2019.

[14] Aras, E., Small, N., Ramachandran, G., Delbruel, S., Joosen, W. & Hughes, D. Selective jamming of LoRaWAN using commodity hardware. Proceedings Of The 14th EAI International Conference On Mobile And Ubiquitous Systems: Computing, Networking And Services. pp. 363-372, 2017.

[15] Le, A., Loo, J., Lasebae, A., Aiash, M. & Luo, Y. 6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach. International Journal Of Communication Systems. 25, 1189-1212, 2012.

[16] Khanji, S., Iqbal, F. & Hung, P. ZigBee Security Vulnerabilities: Exploration and Evaluating. 2019 10th International Conference On Information And Communication Systems (ICICS). pp. 52-57, 2019.

[17] Rahman, R. & Shah, B. Security analysis of IoT protocols: A focus in CoAP. 2016 3rd MEC International Conference On Big Data And Smart City (ICBDSC). pp. 1-7, 2016.

[18] Roselin, A., Nanda, P., Nepal, S., He, X. & Wright, J. Exploiting the Remote Server Access Support of CoAP Protocol. IEEE Internet Of Things Journal. 6, 9338-9349, 2019.

[19] Harsha, M., Bhavani, B. & Kundhavai, K. Analysis of vulnerabilities in MQTT security using Shodan API and implementation of its countermeasures via authentication and ACLs. 2018 International Conference On Advances In Computing, Communications And Informatics (ICACCI). pp. 2244-2250, 2018.

[20] Vaccari, I., Aiello, M. & Cambiaso, E. SlowITe, A Novel Denial of Service Attack Affecting MQTT. Sensors. https://www.mdpi.com/1424-8220/20/10/2932, 2020.

[21] Malik, M., McAteer, I., Hannay, P., Firdous, S. & Baig, Z. XMPP architecture and security challenges in an IoT ecosystem. Security Research Institute, Edith Cowan University, 2018.

[22] Naik, N. Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. 2017 IEEE International Systems Engineering Symposium (ISSE). pp. 1-7, 2017.

[23] McAteer, I., Malik, M., Baig, Z. & Hannay, P. Security vulnerabilities and cyber threat analysis of the AMQP protocol for the internet of things, 2017.

[24] White, T., Johnstone, M. & Peacock, M. An investigation into some security issues in the DDS messaging protocol. 2017.

[25] Boudouaia, M., Ali-Pacha, A., Abouaissa, A. & Lorenz, P. Security Against Rank Attack in RPL Protocol. IEEE Network. 34, 133-139, 2020.

[26] Kara, M. & Furat, M. Client-Server Based Authentication Against MITM Attack via Fast Communication for IIoT Devices. Balkan Journal Of Electrical And Computer Engineering. 6 pp. 88 - 93, 2018.

[27] Milinic, V. Investigating Security Issues in Industrial IoT: A Systematic Literature Review. Mälardalen University, School of Innovation, Design, 2021.

[28] Zhou, L., Guo, H. & Deng, G. A fog computing based

approach to DDoS mitigation in IIoT systems. Computers & Security. 85 pp. 51-62, 2019.

[29] Serror, M., Hack, S., Henze, M., Schuba, M. & Wehrle, K. Challenges and opportunities in securing the industrial internet of things. IEEE Transactions On Industrial Informatics. 17, 2985-2996, 2020.

[30] Zhou, L., Yeh, K., 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. 35, 76-87, 2018.

[31] An, X., Lü, X., Yang, L., Zhou, X. & Lin, F. Node state monitoring scheme in fog radio access networks for intrusion detection. IEEE Access. 7 pp. 21879-21888, 2019.

[32] Hussain, F., Hassan, S., Hussain, R. & Hossain, E. Machine learning for resource management in cellular and IoT networks: Potentials, current solutions, and open challenges. IEEE Communications Surveys & Tutorials. 22, 1251-1275, 2020.

[33] Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M., Al-Turjman, F. & Mostarda, L. Cyber security threats detection in internet of things using deep learning approach. IEEE Access. 77 pp. 124379-124389, 2019.

[34] Xiong, J., Ma, R., Chen, L., Tian, Y., Li, Q., Liu, X. & Yao, Z. A personalized privacy protection framework for mobile crowdsensing in IIoT. IEEE Transactions On Industrial Informatics. 16, 4231-4241, 2019.

[35] Hassanzadeh, A., Modi, S. & Mulchandani, S. Towards effective security control assignment in the Industrial Internet of Things. 2015 IEEE 2nd World Forum On Internet Of Things (WF-IoT). pp. 795-800, 2015.

[36] Sisinni, E., Saifullah, A., Han, S., Jennehag, U. & Gidlund, M. Industrial internet of things: Challenges, opportunities, and directions. IEEE Transactions On Industrial Informatics. 14, 4724-4734, 2018.

[37] Jia, X., Feng, Q., Fan, T. & Lei, Q. RFID technology and its applications in Internet of Things (IoT). 2012 2nd International Conference On Consumer Electronics, Communications And Networks (CECNet). pp. 1282-1285, 2012.

[38] Atzori, L., Iera, A. & Morabito, G. The internet of things: A survey. Computer Networks. 54, 2787-2805 (2010)

[39] Liu, X., Zhao, M., Li, S., Zhang, F. & Trappe, W. A security framework for the internet of things in the future internet architecture. Future Internet. 9, 27, 2017.

[40] Lin, S. Industrial Internet Reference Architecture. Industrial Internet Consortium, 2015.

[41] Arat, F. & Akleylek, S. A Systematic Survey on Mobile Internet of Things Security. 14th International Information Security And Cryptology Conference, 2021.

[42] Taylor, K. 10 Examples of Industrial Internet of Things (IIoT) in Detail. HitechNectar, https://www.hitechnectar.com/blogs/examples-industrial-internet-of-things/, 2021.

[43] Sharma, V., You, I., Andersson, K., Palmieri, F., Rehmani, M. & Lim, J. Security, privacy and trust for smart mobile-Internet of Things (M-IoT): A survey. IEEE Access. 8 pp. 167123-167163, 2020.

[44] Khalil, R., Saeed, N., Masood, M., Fard, Y., Alouini, M. & Al-Naffouri, T. Deep Learning in the Industrial Internet of Things: Potentials, Challenges, and Emerging Applications. IEEE Internet Of Things Journal, 2021.