

We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,100

Open access books available

149,000

International authors and editors

185M

Downloads

Our authors are among the

154

Countries delivered to

TOP 1%

most cited scientists

12.2%

Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com



Artificial Intelligence Deployment to Secure IoT in Industrial Environment

Shadha ALAmri, Fatima ALAbri and Tripti Sharma

Abstract

Performance enhancement and cost-effectiveness are the critical factors for most industries. There is a variation in the performance and cost matrices based on the industrial sectors; however, cybersecurity is required to be maintained since most of the 4th industrial revolution (4IR) are based on technology. Internet of Things, IoT, technology is one of the 4IR pillars that support enhancing performance and cost. Like most Internet-based technologies, IoT has some security challenges mostly related to access control and exposed services. Artificial intelligence (AI) is a promising approach that can enhance cybersecurity. This chapter explores industrial IoT (IIoT) from the business view and the security requirements. It also provides a critical analysis of the security challenges faced by IoT systems. Finally, it presents a comparative study of the advisable AI categories to be used in mitigating IoT security challenges.

Keywords: artificial intelligence, Internet of Things, cybersecurity, industry, industrial IoT (IIoT), 4th industrial revolution

1. Introduction

The 4th Industrial revolution (4IR) is the current era where industry is driven by technology. It encourages the co-operation between scientific knowledge and experience with business mindset and requirements. The key technologies that allow 4IR to be sustained are additive manufacturing techniques, Autonomous and collaborative robotics, Industrial Internet of Things (IIoT), Big data analytics, Cloud Manufacturing techniques [1]. The current scenarios show the benefits of IIoT in improving QoS industries, starting from predictive maintenance, reaching remote controlling of assets, and deploying Digital Twin concept that allows virtualizing the operations environment and permits the owner to be proactive when any anomalies are detected [2]. Even though IIoT adds value to the traditional industry, there should be a balance between the operational benefits and the security level.

Aims and objectives

- To study and compare the existing IoT architectures

- To explore industrial IoT (IIoT) from the business point of view
- To analyze various IIoT threats and security challenges and existing mitigation techniques
- To perform a comparative study of the different AI categories and their applicability in IIoT security
- To recommend the most convenient AI techniques for mitigation of IIoT security challenges

This chapter is designed to be used as a reference to study the effectiveness of Artificial intelligence (AI) and to enhance the security techniques for mitigating the threats faced by IIoT deployment. Section 2.1 discusses IoT architecture and Section 2.2 demonstrates the IoT security challenges. Section 2.3 describes the main AI categories and their subcategories. It also points out the appropriate and relevant situation to employ AI categories based on the available data and the type of intelligence needed. Section 3 explores IIoT details, its significant business model, and the added values. Section 4 focuses on IoT security in terms of threat model, threats classification, and common IoT security mitigations. This chapter ends with a comparative study of AI categories used to mitigate IIoT security challenges in Section 5.

2. Background

2.1 IoT architecture

Internet of Things (IoT) is a service-oriented paradigm that is built on the involvement of several technologies. Therefore, its architecture consists of layers starting from sensors and reaching to constructive data displayed on the system-analyzer screen.

In References [3–5], the main IoT architecture consists of devices that have sensors and edge computing which has embedded devices, fog computing such as gateway and servers, cloudlets such as base stations, and the last component being cloud computing, which can be any cloud platform. **Table 1** shows some IoT architectures with variations on the number of layers based on five different references. In general, there are three main layers that are devices, network, and cloud computing. However, the device layer can be divided into two sub-layers based on the type and functionality: The first sub-layer comprises of end-user devices that contain sensors; and the second sub-layer are devices that support machine-to-machine communication such

Ref	Number of layers	Layers title
[3]	5 layers	Devices, edge Computing, fog computing, cloudlets, cloud computing
[4]	3 layers	IoT layer, fog layer, cloud layer
[5]	3 layers	EoT(ecosystem of Things) layer, edge layer, cloud layer
[6]	4 layers	Fog network consist of (IoT layer, Mist, cloudlet/edge layer,) cloud
[7]	4 layers	Sensors and systems layer, far edge layer, near-edge layer, cloud layer

Table 1.
IoT ecosystem architecture comparison.

as an Arduino platform. The network layer can be divided as well into two sub-layers based on the communication characteristics such as the speed and bandwidth: fog computing and cloudlet. The third layer is the cloud computing layer. **Figure 1** illustrates the authors' insights into IoT architecture after studying the literature. Layer one consists of IoT devices, layer two covers all networking related technologies and devices, and the third layer consists of cloud computing and related data analytics technologies.

The IoT layers are connected through networking media using wireless or wired connections. However, wireless technology evolution is critical to extend IoT deployment as the complexity of energy impact and processing capacity are getting worse at the sensor's layer [6]. The emerging of 5G in wireless communication adds an advantage to IoT architecture since it improves the performance by allowing the transformation of more data in less time, which technically reduces service-latency and enhances real-time access to data [6, 8].

2.2 IoT security challenges

The growing use of Internet of Things (IoT) technology in the industrial sector has posed new issues for the device and data security. Based on different world statistics, the number of devices connected to IoT networks is rapidly increasing. This expansion leads to experience different levels of vulnerabilities, which may—in turn—cause an increase in security threats and challenges. Security may be regarded as a big threat that leads to limitations of the IoT systems deployment. As a result thereof, it is the Authors' view that effective security practices may become more vital in the IoT industry.

The National Institute of Standards and Technology (NIST) designed programs to boost cybersecurity involvement in IoT [9]. This initiative promotes the development and implementation of cybersecurity standards, guidelines, and tools for IoT products, connected devices, and their deployment environment.

- Security Challenges: Some common challenges posed by the security requirements for the IoT systems are given as follows:
 - Because IoT involves various and diverse technologies, determining and understanding security needs is more complicated.

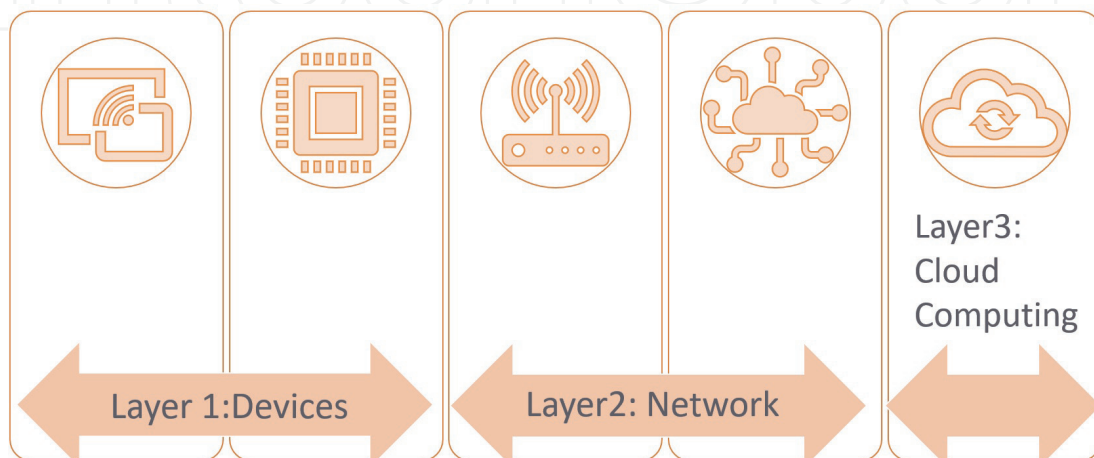


Figure 1.
IoT architecture.

- IoT networks typically consist of resource-constrained devices. Therefore, these devices became the weakest link for cyberattacks.
- The Internet of Things (IoT) may include mobile devices that demand adaptability, posing security vulnerabilities.
- IoT also generates a vast amount of data, which is referred to as Big data. The latter has its own set of security and management concerns.
- Security requirements: Because of the varied nature of IoT Applications, security requirements may also differ. Based on the scenarios from a specific industry and the infrastructure to which IoT is being applied to, the requirements and consequent security measures may be changed or adjusted. Nevertheless, the common security requirements [10–13] of IoT systems can be summarized as given in **Table 2**.

Satisfying all the above-mentioned requirements is a huge challenge because of the limitations and constraints associated with the IoT devices in terms of capability and capacity to deploy the conventional security solutions.

2.3 Artificial intelligence categories

When it comes to artificial intelligence (AI), there are several philosophical groundworks that have been done. As per Russel [14], there are two types of AI: weak AI where machine can act intelligently and strong AI where machine can really think. However, when hybrid mechanisms are used, the deployment of AI system features is enhanced.

Artificial intelligence (AI) can be divided into two main categories as per the mechanisms that are used to reach intelligence through data processing [14–16]. The

Security requirements	Example of mitigation techniques	Requirement description
Confidentiality	Encryption	Only authorized entities should be able to read it to ensure data protection.
Integrity	Hash generation	The data should be checked to ensure that it has not been tampered with.
Authentication, Authorization, Access control (AAA)	Implement policies, Security credentials, firewall, and authentication servers. Digital signature, etc.	<ul style="list-style-type: none"> • Identification of devices and users. • Special rights or privileges for authorized users; • Access to resources and data should be restricted.
Availability	Fault tolerance mechanism, clustering and high availability architecture, etc.	The ability to be accessed and used by an authorized entity on demand
Non-repudiation	Digital signature	Securing information transmission by supplying confirmation of delivery and identification to both sender and receiver so that neither can later deny processing it. It ensures data origin and integrity.

Table 2.
IoT security attributes, techniques and requirements.

first category is knowledge-based in which the main component is the existence of inference engine, and it is known as expert system (ES). The second category is machine learning (ML) where different algorithms are used to allow the machine to learn from the dataset. **Table 3** illustrates the main AI categories. The core element is knowledge engineering in order to build either the dataset for ML or the fact database for ES. The data preparation phase needs to make use of other technology such as data mining and Big data techniques. The ML sub-categories are supervised learning, reinforcement learning, and un-supervised learning. The ES types of systems are rule-based, Fuzzy-logic, and frame-based.

- **Machine Learning types (ML):** The intelligence behind ML is the ability to learn. ML involves adaptive mechanisms; therefore, it is considered as the basis of adaptive systems. In this context, the ML detects and extrapolates patterns by adapting to new circumstances. This learning process can be based on experience or examples or analogy. Therefore, ML has three sub-categories as follows:
 - **Supervised learning:** is learning from examples. This type is the easiest ML type in terms of mathematical complexity. The machine learns from *a behavior (labels)*.
 - **Reinforcement learning:** defined as learning from the environment based on experience. This type is based on an agent that can learn from *reward signal*. The machine learns from its mistake.
 - **un-supervised:** referred to as learning based on analogy and to find a pattern from a dataset. This type is used when there are no examples to learn from and no reward signal to get feedback.

Figure 2 shows examples of mechanisms for each ML sub-category.

- **Expert System (ES):** The Expert System, ES is dealing with uncertain knowledge and reasoning. Rule-based ES consist of five basic components that are shown in **Figure 3:** the knowledge base, the database, the inference engine, the explanation facility, and the user. ES intelligence resembles the way the expert human apply their knowledge and intelligence to solve the problem in a narrow domain. ES processes knowledge in the form of rules and uses symbolic reasoning to solve the problem. The main difference between ES and conventional programs (CP) is that the CP processes data using algorithms on well-defined operations to solve a problem in a general domain. Examples of ES are as follows:

Expert system (ES)	Machine learning (ML)
Rule-based	Supervised learning
Fuzzy logic	Reinforcement learning
Frame-based	Un-supervised Learning

Table 3.
 Artificial intelligence (AI) main categories.

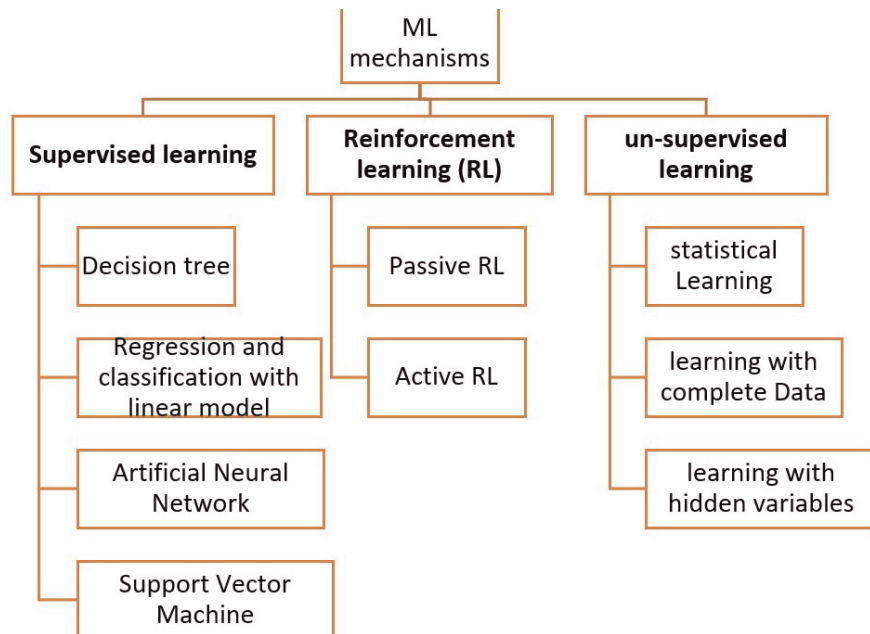


Figure 2.
Examples of ML sub-categories mechanisms.

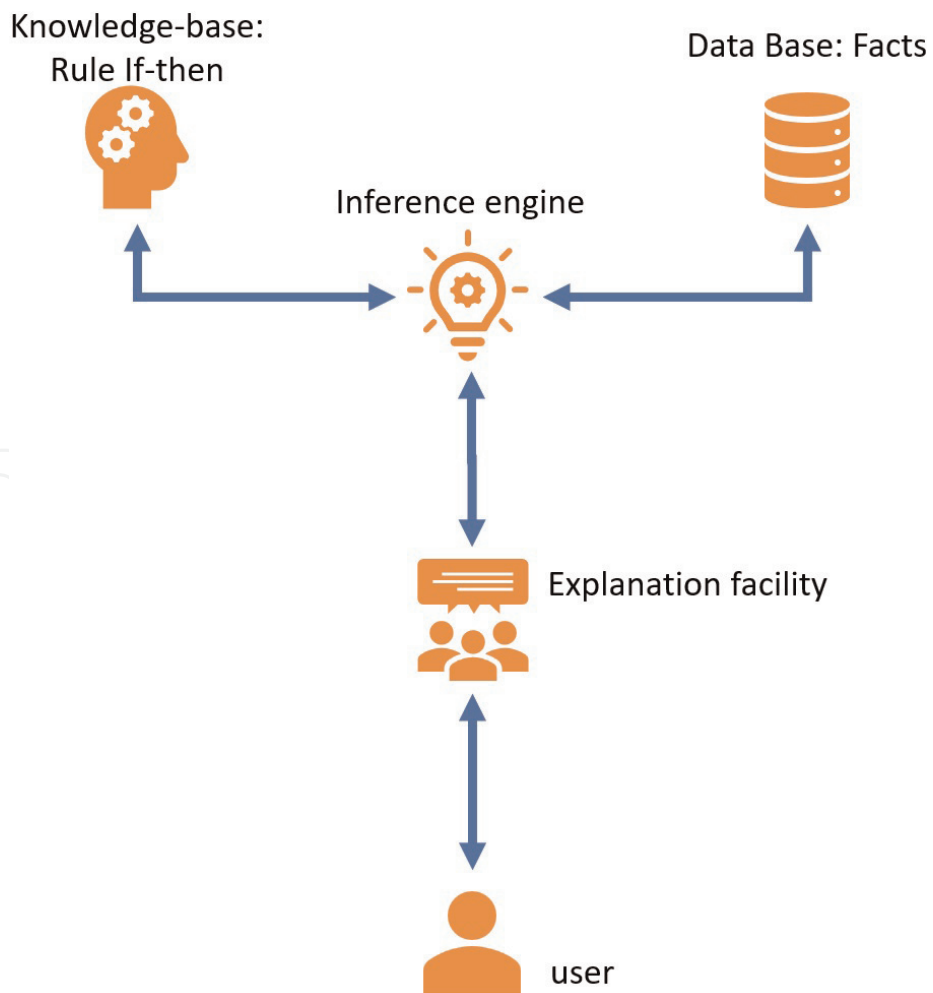


Figure 3.
Expert system (ES) rule based adapted from [15].

- **Rule-based:** is based on logical rules. Its disadvantage comes from ineffective search strategy and inability to learn.
- **Fuzzy logic:** is centered on logic that describes fuzziness. It models the common sense of a human. Tuning is the most ponderous stage of building a fuzzy system.
- **Frame-based:** is constructed on structuring knowledge based on object attributes. It usually uses pattern matching but it has a limitation to make decisions about the hierarchical structuring during knowledge engineering.

3. Artificial intelligence in industrial IoT

3.1 The significance of AI in IIOT

Artificial intelligence (AI) deployment in Industrial IoT (IIoT) systems is very convenient due to the huge data generated by the IoT system. AI approaches are used to infer knowledge and support data analytics. The main areas requiring exploration and proposing solutions for intelligent IIoT systems are threat hunting and intelligence, blockchain, edge computing such as cloud computing, privacy preservation [17].

The generated big data from IIoT are due to real-time computation and the risk increases when the communicated data are critical and sensitive; therefore, AI can support the need of big data analysis with low latency [2]. Designing security and privacy solutions require to identify business processes and operations. However, this task is complex in the regular industrial system, and it comes more sophisticated in IIoT [18]. AI technology deployment has several implementations including computing paradigm and security; however, inter-operability issues are regarded as a critical challenge [3].

The Internet of Things (IoT) has grown from a concept used in research laboratories and technology companies to a reality in everyday lives. IoT has become embedded in the operations of some companies, enterprises, and governments [19]. Emerging IoT applications are spread out in all domains, and it has affected a variety of industries. **Figure 4** illustrates the examples of IoT technology applications, which include Smart Homes, Smart Health, Intelligent Transportation, Smart Cities, Smart Agriculture, and Factory Automation [3].

Indeed, the very same report by McKinsey & Company mentioned above [19] identifies the top five sectors where IoT adds the most economic value: factories that include all standardized production environments followed by human health, work sites, cities, and retail environment. Indeed, it has been estimated in this report that IoT could add a value of \$5.5 trillion to \$12.6 trillion by 2030, where the most value can be created in B2B type of applications.

3.2 The IoT business model

The term business model describes how an organization creates, delivers, and captures value [20]. The adoption of IoT technologies in an organization will most certainly affect the business relationships and the business model for that organization. In this section, the common business models used will be discussed.

One of the early initiatives to develop an IoT business model was published in 2015 [21]. The research focused on identifying the relevant building blocks that can fit in

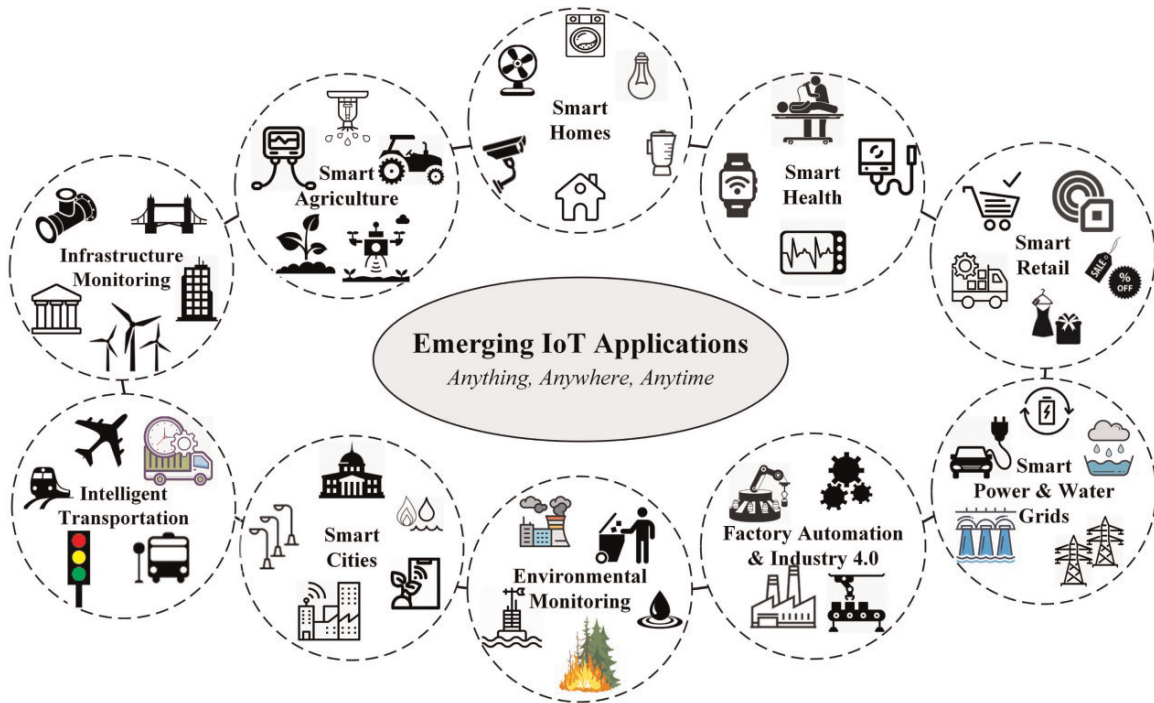


Figure 4.
Example of industry utilizing IoT technology [3].

IoT business models, as well as the types and importance of the building blocks. This framework identified value proposition as the most important building block for IoT business models. The entities “customer relationships” and “key partnerships” followed suit in terms of importance.

Another conceptual IoT Business Model is the AIC (Aspiration, Implementation and Contribution) model presented in [22], which focuses on context-specific implementation of IoT. This model consists of three interconnected phases: Aspiration, Implementation, and Contribution. The first phase “Aspiration” focuses on defining and predicting the value creation through adoption of IoT. The second phase Implementation includes strategy development in which an organization should investigate how IoT will improve the business by gaining competitive advantage or creating enhanced products or services. In the third phase Contribution, an organization opting for IoT should study the practicality of the approach and the capabilities and resources available for the organization to implement IoT. In other words, does the organization own the knowledge and skills needed to succeed in implementing IoT.

Four types of IoT-enabled servitized business models were classified in [23]. Each business model was analyzed from three perspectives: the role of IoT, the firm’s benefits, and the inhibiting factors. **Table 4** adapts from the study presents the four types of IoT business models and compares them based on the stated three perspectives. The four different business models have some shared features as the common role for IoT is adaptation, the common benefit is reducing operation cost, and the common inhibiting factor is the need for close relationship between different stakeholders.

IoT business models vary based on the type of deployment. Therefore, each industry has a different model that will fit with its value proposition. Seven IoT business models were reviewed by the researchers in [24]. Based on their analysis, six characteristics of the IoT business model were identified:

IoT Business model	Role of IoT	Firm's benefits	Inhibiting factors
Add-on business model	<ul style="list-style-type: none"> • Innovation • Adaptation • Smoothing 	<ul style="list-style-type: none"> • Improve product-service offerings • Extend firms business • Reduce operation costs 	<ul style="list-style-type: none"> • Privacy concerns • Data security • Requires close relationship between different stakeholders in the network
Usage-Based business model	<ul style="list-style-type: none"> • Adaptation • Smoothing 	<ul style="list-style-type: none"> • Extend firms business • Generate steady income • Reduce operation costs 	<ul style="list-style-type: none"> • Requires expertise in data management • Requires close relationship between different stakeholders in the network
Sharing business model	<ul style="list-style-type: none"> • Adaptation • Smoothing 	<ul style="list-style-type: none"> • Improve service offerings • Increase resource utilization • Reduce operation costs 	<ul style="list-style-type: none"> • Requires new ways of interactions with customers • Requires close relationship between different stakeholders in the network
Solution-oriented business model	<ul style="list-style-type: none"> • Innovation • Adaptation 	<ul style="list-style-type: none"> • Extend firms business • Gain competitive advantage • Reduce operating cost 	<ul style="list-style-type: none"> • Developing servitized offerings that aligns with customer's needs • Requires close relationship between different stakeholders in the network

Table 4.

Business model categorization based on role, benefits, and inhibiting factors.

- The ability to capture the transition between different business models.
- The possibility to connect IoT elements to the business model components.
- The ability to view the relation between business-centric and a network-centric approaches.
- The ability to map the Value Flows that involve revenue, costs, and assets
- The possibility to include the model patterns of digital business.
- The ability to balance between the actions and widening the rational thinking.

3.3 Analytical study of how IoT add-value to the industry

Given the potential impact and IoT devices' prevalence and ubiquity, one needs to understand how to leverage IoT technologies to realize the value-deriving benefits associated with them. For example, IoT can be used in the factory setting to make various processes more efficient. The IoT applications have noteworthy potential in value creation in terms of operation optimization and predictive maintenance. This can be achieved by monitoring, remotely tracking and adjusting the machineries, based on sensor data from different parts of the factory. It has been estimated that IoT

has a potential to create value of \$1.2 trillion to \$3.7 trillion per year in 2025 by optimizing factory settings. This improvement in the working efficiency using IoT may also induce some security and privacy issues [25]. Moreover, technology does not automatically bring added convenience or value unless firms carefully consider the context into which it is introduced and how to derive any practical or monetary benefits. Mostly, add-value is related to performance enhancement. The latter can be improved through a variety of factors such as time saving, cost saving, and processing low-overhead to name but a few.

Table 5 shows some recent empirical research [26–31] on how to mitigate security challenges in an IoT industrial environment and different add-value. AI approaches are used more in access control, which is related mostly to the Network layer of IoT. Access control is a critical part of the system, which acts as a door for the factory to control authorized access to the resources and the level of privileges. Due to the heterogeneous and dynamic nature of the IoT networks, it will be significant to use AI approaches to enhance the access control.

The IoT add-value is constraint by several challenges and barriers. These can be categorized in two groups based on their domain as follows:

- Human limitations
- lack of social acceptance and knowledge
- lack of skilled workforce, technical knowledge
- Technology limitation
- the absence of technical accountability and regulation
- challenges related to data management and data mining
- privacy, security, and uncertainty

Ref.	IoT layer	Security mitigation approach	Performance (add-value)	AI used
[26]	Network	Graph-theory	Cost is not evaluated Different performances based on number of nodes	×
[27]	Data (access control)	Conditional proxy re-encryption primitive	Low overhead	×
[28]	Data (access control)	Context-aware analysis	Improve detection ration	×
[29]	Network	Deep Learning and Blockchain-Empowered Security Framework	Standard measures of latency, accuracy, and security	✓
[30]	gateways	Flexible rule-based control strategies	Cost and time saving	×
[31]	Network	A deep learning methodology for detecting cyberattacks	Improve detection accuracy of IDS	✓

Table 5.
Examples of AI usage in security mitigation approaches based on IoT layer.

- the immaturity of IoT innovations
- integration among networks and no standardization of regulations
- Business limitation
- difficulty in designing business models for the IoT due to a multitude of different types of connected products
- ecosystems are unstructured since it is too early to identify stakeholders and their roles

Uncertainty of how IoT will impact existing business models, organizational strategies, and return of investment, business models are considered significant barriers to implementation, where the add-value should be clearly identified.

4. Critical analysis of IoT security

4.1 Threat modeling

A threat model is an essential approach in defining security requirements. The goal of threat modeling is to understand how an attacker would be able to compromise a system, and then to ensure that proper mitigation techniques are in place to prevent such attacks. Threat modeling pushes the design team to consider the mitigations during the process of the system creation before deployment. In general, the threat modeling process consists of four steps.

- step 1: Model the application
- step 2: Recognize and Enumerate Threats
- step 3: Use countermeasures to Mitigate threats
- step 4: Verify and validate the mitigations

The most critical step is step 2 aimed at exposing the vulnerabilities and security challenges of the IoT systems. After properly classifying the threats, it will be possible to explore the mitigation techniques. For classifying threats in an information system, Microsoft introduced the STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service and Elevation of privilege) threat model [32] Countermeasures are recommended and evaluated for each threat. The application of STRIDE for threat modeling in Industrial IoT (IIoT) has been studied before as discussed in [33, 34]. It also describes the adaptation of STRIDE for the Azure IoT reference architecture. After discovering threats, these should be rated according to their severity using some tools. The use of the DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability) model as one of commonly used tools to assign ratings to threats is mentioned in [35].

Generally, each IoT system will have a multi-layered architecture consisting of various layers. These layers make use of diversified technologies, which introduce a

plethora of challenges and security threats. As a result, the architecture of the IoT system plays a significant role in identifying the threats and attacks. However, there is no specific standard architecture because most of the IoT solutions are application-specific developed with explicit technologies, resulting thus in heterogeneous and fragmented architectures.

A secured IoT network architecture was proposed in [36] that would be using Software Defined Networks (SDN) for identifying the threats. It also summarizes how IoT network security can be achieved in a more effective and flexible way using SDN. Furthermore, studies, reviews, and analysis were conducted on some existing IoT architectures and a new architecture was proposed based on those architectures [37]. This new architecture includes a lot of the key elements of the other architectures, while fostering a high degree of inter-operability across diverse assets and platforms. Among the several IoT architectures reviewed in [38], it is found that the four-layer architecture (Application, Transport, Network, and Perception layers) is often being considered by researchers to address security challenges and solutions at each layer. Moreover, the most used IoT architectures are often three-tier/layer systems, including a perception/hardware layer, network and communication layer, and application interfaces and services layer. Additionally, the Open Web Application Security Project (OWASP) [39] identified attack vectors using the three layers of an IoT system: hardware, communication links, and interfaces/services layers. Thus, as shown in **Figure 5** at all layers of the IoT architecture, implementation of IoT security mitigation techniques should include security architecture [40].

According to the IoT security architecture, there are security issues and concerns at each of the three IoT layers. Because of their relative positions in the architecture, each of these layers has its own set of security needs. However, because they are all interconnected, if one is compromised, the others may suffer as well. The goal of IoT security is to protect customer’s privacy, confidentiality, data integrity, infrastructure, and IoT device security, as well as the availability of the services. The following subsection discusses the IoT Security issues and threats at each of the layer.

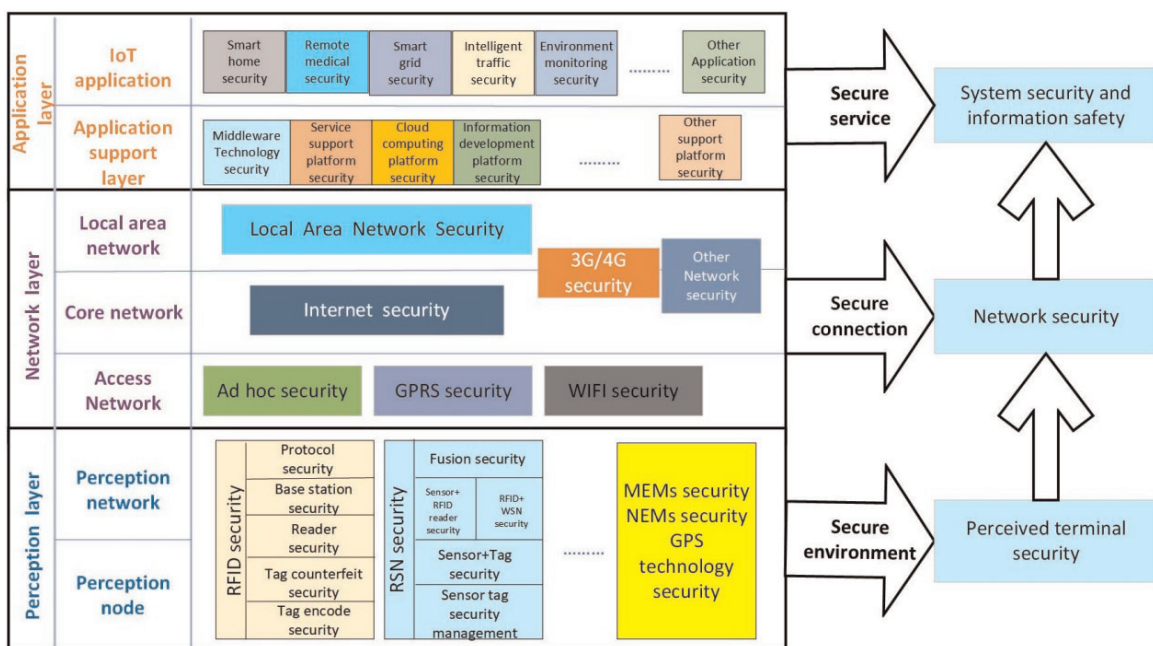


Figure 5. IoT security architecture [40].

4.2 Classification of IoT threats and attacks with solutions

Like in any other system, confidentiality, integrity, AAA, availability, and non-repudiation are some general security goals and requirements as already stated in previous sub-section. This section discusses about some of the most frequent threats and attacks at each IoT layer that might affect at least one of these criteria. Following **Table 6** provides an overview of the classification of the threats at each IoT layer and some proposed solutions corresponding to these threats [41–44].

4.3 State-of-art IoT security mitigations

The primary goal of implementing security mitigation is to ensure privacy, confidentiality, and the security of IoT users, infrastructures, data, and devices, as well as to ensure the availability of services provided by an IoT ecosystem. As a result, mitigation and countermeasures are often implemented in accordance with the traditional threat vectors.

In the above sub-section, some empirical based solutions have been listed in **Table 2** corresponding to the given threat or attack. Based on the studies performed in [11, 45–47], it is observed that some ubiquitous state-of-the-art technologies such as Blockchain, Fog Computing, Edge Computing, SDN, Artificial Intelligence can be used to enhance the security in an IoT environment. These technologies are vital and have enormous potential for addressing the IoT ecosystem's security concerns.

Blockchain (BC): A blockchain is a special kind of database. It differs from a standard database because of the unique approach in which it saves data. Data are, hence, saved in a series of blocks that are subsequently linked together to form a blockchain. IoT devices capture data from sensors in real time, and BC provides data security by establishing a distributed, de-centralized, and shared ledger [48]. Due to its critical operational properties, such as distributed functionality, de-centralized behavior, encrypted communication, embedded cryptography, and authorized access, it provides security solutions against a variety of threats across the different layers of the IoT such as disclosure of critical information, device compromise, malicious data injection, tag cloning, node cloning, unauthorized access, software modification, data manipulation, spoofing, session hijacking, false data injection, brute force attack.

Fog computing (FC): Fog computing allows processing, storage, and intelligent control to be close to the data devices themselves. Hardware failures, eavesdropping, device compromise, disclosure of critical information, leaks of critical information, node tampering, node capture attacks, node replication, battery drainages attack, illegal access, DoS and DDoS, MITM, etc. are just some of the threats and attacks that can be prevented by the vast processing, storage and management capabilities of the voluminous data that it processes, stores, and manages.

Edge Computing (EC): In edge computing, data are transmitted within the network or within the device. Data movement is reduced as compared to fog computing, which alleviates security concerns. Real-time services such as intrusion detection, identity recognition, access management enable edge computing to strengthen security against a variety of threats and attacks, including battery drain, hardware failure, eavesdropping, node capture, DoS and DDoS, SQL injection, jamming, malicious attack, virtualization, data integrity, cloud flooding attack, illegal access.

SDN: Software-defined networking is the preferred method of managing network security in a variety of application domains, including smart homes, businesses, and e-health care systems. The control plane and data plane refer to the two primary tasks

Layer	Threats/ attacks	Description	Solution
Perception Layer	Eavesdropping	An intrusion, also known as a sniffing or spying attack, occurs when someone attempts to steal information sent by the devices.	Deploying intrusion detection system.
	Replay Attack	An intruder listens to the transmission between sender and receiver and steals legitimate data from the sender.	Using one-time passwords and session keys and timestamps
	RF Jamming	RFID tags may potentially be exploited via a DoS attack, when RF transmission is disrupted by excessive noise signals.	Encryption & authentication.
	Node Capture	An attacker takes control over a key node, like a gateway node to use its resources.	Authentication and access control.
	Fake Node and Malicious	It is a kind of attack in which an attacker modifies the system by adding a node and injecting bogus data. This created node drains vital energy from genuine nodes and may gain control of them, thus destroying the network.	Authentication and access control.
Network Layer	Sybil Attack	In this attack, the attacker controls and changes the node in such a way that it shows multiple identities, hence compromising a huge portion of the system and resulting in misleading information about redundancy.	Trusted certificates that are based on a central certification authority.
	Sinkhole Attack	The attacked hole serves as a strong node, and so other nearby nodes and devices prefer it for communication or as a forwarding node for data routing, and thus acts as a sinkhole, attracting everything.	Intrusion detection system, strong authentication techniques.
	Denial of Service (DoS) Attack	This kind of attack causes the targeted system's resources to be exhausted, rendering the network inaccessible to its users because of an attacker's flood of useless traffic.	Configuring a firewall which denies ping requests or using AES encryption.
	Man-in-the-Middle Attack	Using a middleman attack, the attacker pretends to be the original sender, making the recipient believe that the message came from them.	Using high level encryption and digital signatures.
	RFID Spoofing	These attacks are designed to transfer malicious data into the system by gaining access to the IoT system. RFID spoofing, IP spoofing, and other spoofing attacks in IoT systems are examples.	RFID Authentication protocols.
	Unauthorized access	An unauthorized person may get access to the IoT device over the network.	Authentication and access control.
Application Layer	Malicious Code Attacks	This attack is done by executing the malicious scripts or code. It is a hacking method enabling the attacker to first insert the malicious code into the system and then data is stolen from the user by executing these malicious scripts.	Firewall is inspected at run time.

Layer	Threats/attacks	Description	Solution
	Cross site scripting	Client-side scripts, such as javascript, may be injected into a trusted website by an attacker. An attacker may then totally alter the application's content to suit his requirements and illegally use original data.	Validating user input and the input by the web page.
	Phishing attack	The attacker spoofs the legitimate users' data to get their usernames, email addresses, and passwords. The attacker creates a false e-mail or website, and then the legitimate user logs in, stealing their data.	Using anti-phishing, prevention techniques.
	Botnet	By using a botnet, the hacker may take over a network of devices and control them from a single access point.	Using a secure router encryption protocol, such as WPA2.
	SQL injection	SQL script is used to log into the IoT Devices and applications.	Programming the log page using parameterized statements.

Table 6.
 Common IoT threats, description, and solutions.

of switches/routers. The control plane determines where traffic should be routed, whereas the data plane routes traffic to a specific destination. The control plane and data plane are linked together in conventional networking, but are separated in an SDN architecture. The data plane runs on hardware, while the control plane runs on software and is logically centralized. SDN is capable of monitoring and detecting harmful activity on the network. It separates the compromised nodes from the rest of the network by identifying them. Flow statistics in SDN architectures was employed to detect anomalies through a variety of techniques, including DDoS attacks, port scanning, and worm spreading [49].

Artificial intelligence (AI): The use of artificial Intelligence is growing in cybersecurity because it can help protect systems from cyber threats in a more dynamic way. AI is most frequently employed in cybersecurity for intrusion detection, which involves studying traffic patterns and looking for activities indicative of threat. With the growth of IoT technology, AI has received considerable attention. As a result of this expansion, AI technologies such as machine learning, support vector machines, decision trees, linear regression, and neural networks have been integrated into IoT cybersecurity applications to detect threats and prospective attacks. AI is viable for IoT security, particularly for the four critical risks: intrusion detection, defense against DoS/DDoS attacks, device authentication, and virus detection [50]. The following section discusses the role of AI techniques and their comparative studies for IoT security.

5. Comparative study AI categories used to mitigate industrial IoT security

AI is a promising approach, which can be employed to mitigate the security challenges faced by IoT autonomous system. As per [51], the secure solution can be

improved through AI approaches to predict future threats. The researchers point out generative adversarial networks (GAN) that are using generator and discriminator. The generator's scope is to add samples to the real data, whereas the discriminator's purpose is to remove the fake samples from the original data. The suggested AI-based solutions are from the data-driven type, which are support vector machine (SVM), neural networks (NN), artificial neural networks (ANN), recurrent neural network (RNN).

A framework has been proposed where AI based reaction agent is introduced [52]. The security enhancement is a combination between two intrusion detection systems: knowledge-based and anomaly-based. For network pattern analysis, Weka has been used as data mining tool and NSL KDD as dataset source and distributed JRip algorithm in which machine learning can be used for security enhancement. For anomaly-based IDS, the dataset is collected from real sensor data and the model uses library of python Scikit-learn.

The main finding of [53] is that AI can be used for IoT security mostly in intrusion detection system (IDS) in order to analyze the traffic and learn the characteristic of the attack. Naïve Bayes algorithm is mostly used to classify attack data where it is assumed this to originate from the independent events.

A two-tier framework is proposed by [54] for embedded systems such as an IoT system. The security mitigation is to improve the traditional host-based IDS. The machine learning approach used is of a pipeline method where a set of algorithms are involved which allow the flexibility of adjusting the ML processing and the link between different tiers.

From a comprehensive survey published by [55], it has been found that high-level encryption techniques are not advisable to be implanted in IoT systems due to resource limitation. Therefore, AI approach is a very strong candidate to enhance security in IoT system in addition to the other existing network security protocols. Consequently, to the nature of IoT-layered architecture, each layer has its specific security threats. It has been noticed that machine learning approaches are widely adopted in comparison to the knowledge-based expert systems.

Reference	Expert system	Machine-learning	Security mechanism to be enhanced
[51]	✓	✓	DoS, Sybil detection, intrusion detection, MITM, malicious node
[52]	✓	✓	intrusion detection system (IDS)
[53]	✓	✓	Mostly used in (IDS) and MITM
[54]		✓	Host-based IDS
[55]	✓	✓	Different layers of IoT system threats
[56]	✓	✓	IDS
[45]	✓	✓	Authentication mechanisms (Access control) and detection systems
[57]	✓	✓	False Data detection
[58]	✓	✓	IT trustworthiness (safety, security, privacy, reliability, and resilience)

Table 7.
AI branches used in IoT security solutions.

Another study published by [56] suggests that the machine learning based security approaches are used mostly to enhance the detection mechanism of IDS. The only approach that provides mitigation features is based on the techniques that utilizes deep learning such as Gaussian mixture, SNN, FNN, RNN or utilize supervised machine learning such as SVM. **Table 7** [45, 51–58] shows that machine learning is mostly used in the security mechanisms in IoT environment as there are a huge data to learn from.

As per the literature, AI-based methods are recommended to be used to enhance protection against IoT attack. However, most of them are not yet commercialized due to the difficulty of its implementation. The focus of proposing different IoT security mitigation is to introduce high-performance approaches with low cost in a real-time environment. Moreover, dataset preparation is a critical factor that affects the accuracy and efficiency of machine learning approaches.

6. Conclusions

As discussed in this chapter, industries deployed IoT technology to develop industrial applications to add values to their businesses and consumers in terms of performance and cost. Different business models are also reviewed to comprehend that the standardization of IoT business model is very difficult due to the different types of industries and their varied requirements. As such, it is critical for industries to ensure confidentiality, data integrity, availability to ensure data privacy, and security of the system. However, maintaining privacy and security emerged as a challenge in IIoT because of the sophistication of the IoT system. This chapter considered the most used three-layer IoT architecture to study and review the various possible threats and attacks and their conventional mitigation techniques. Conventional security mechanisms have a limitation in IIoT, particularly in predicting attacks.

The state-of-the-art technologies such as Blockchain, Fog computing, Edge computing, SDN, and AI have also been discussed to enhance the security levels in IIoT systems. But artificial intelligence (AI) has been emerging as a promising approach to secure the IIoT-based systems because of its ability to learn from the big data. It furthermore supports data analysis and enhances security mechanisms. AI techniques such as SVM, NN, ANN, RNN have been reviewed and recommended to design and improve countermeasures such as IDS. Data engineering is a critical phase to prepare the datasets required for machine learning. Therefore, it is highly recommended to consider this phase in order to achieve an effective AI deployment. Based on the analysis presented herein, it is the authors' view that this is an open challenge to enhance security mechanisms through AI-based mitigation techniques.

Acknowledgements

We would like to extend our appreciation to the Ministry of higher education and research and innovation for funding this research through the block funding program. This paper is aimed at contributing and further fostering the quality of research in the University of Technology and Applied Sciences in Oman. We extend our gratitude to the reviewers for their insights on the submitted manuscript that greatly improved the chapter.

Glossary of terms


AI	Artificial Intelligence
ML	Machine Learning
QoS	Quality of Services
ES	Experts System
B2B	Business to Business
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service and Elevation of privilege
DREAD	Damage, Reproducibility, Exploitability, Affected Users, Discoverability
SDN	Software-Defined Networks
OWASP	Open Web Application Security Project
Digital Twin:	A digital twin is a virtual representation of an object or system that spans its lifecycle, is updated from real-time data, and uses simulation, machine learning and reasoning to help decision making.

Author details

Shadha ALAmri*, Fatima ALAbri and Tripti Sharma
University of Technology and Applied Sciences, Muscat, Oman

*Address all correspondence to: shadha-alamri@hct.edu.om

IntechOpen

© 2022 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

References

- [1] Bécue A, Praça I, Gama J. Artificial intelligence, cyber-threats and industry 4.0: Challenges and opportunities. *Artificial Intelligence Review*. 2021; **54**(5):3849-3886. DOI: 10.1007/S10462-020-09942-2/FIGURES/3
- [2] Shojafar M, Mukherjee M, Piuri V, Abawajy J. Guest editorial: Security and privacy of federated learning solutions for industrial IoT applications. *IEEE Transactions on Industrial Informatics*. 2022;**18**(5). Available from: <https://ieeexplore-ieee-org.masader.idm.oclc.org/document/9619939/>. [Accessed: February 11, 2022]
- [3] Swamy SN, Kota SR. An empirical study on system level aspects of Internet of Things (IoT). *IEEE Access*. 2020;**8**: 188082-188134. DOI: 10.1109/ACCESS.2020.3029847
- [4] Whaiduzzaman M, Mahi MJN, Barros A, Khalil MI, Fidge C, Buyya R. BFIM: Performance measurement of a blockchain based hierarchical tree layered fog-IoT microservice architecture. *IEEE Access*. 2021;**9**:106655-106674. DOI: 10.1109/ACCESS.2021.3100072
- [5] Chao L, Peng X, Xu Z, Zhang L. Ecosystem of things: Hardware, software, and architecture. *Proceedings of the IEEE*. 2019;**107**(8):1563-1583. DOI: 10.1109/JPROC.2019.2925526
- [6] Oteafy SMA, Hassanein HS. IoT in the fog: A roadmap for data-centric IoT development. *IEEE Communications Magazine*. 2018;**56**(3):157-163. DOI: 10.1109/MCOM.2018.1700299
- [7] Arena F, Pau G. When edge computing meets IoT systems: Analysis of case studies. *China Communications*. 2020;**17**(10):50-63. DOI: 10.23919/JCC.2020.10.004
- [8] Mishra D, Zema NR, Natalizio E. A high-end IoT devices framework to foster beyond-connectivity capabilities in 5G/B5G architecture. *IEEE Communications Magazine*. 2021;**59**(1):55-61. DOI: 10.1109/MCOM.001.2000504
- [9] Fagan M, Marron J, Brady KG Jr, Cuthill BB, Megas KN, Herold R, et al. IoT device cybersecurity guidance for the Federal Government. NIST. 2021; **800**:213. Available from: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-213A.pdf>. [Accessed: February 9, 2022]
- [10] Almtrafi S, Alkhubadi B, Sami G, Alhakami W. Security threats and attacks in Internet of Things (IOTs). *International Journal of Computer Science & Network Security*. 2021;**21**(1):107-118. DOI: 10.22937/IJCSNS.2021.21.1.15
- [11] Krishna RR, Priyadarshini A, Jha AV, Appasani B, Srinivasulu A, Bizon N. State-of-the-art review on IoT threats and attacks: Taxonomy, challenges and solutions. *Sustainability*. 2021;**13**(16): 9463. DOI: 10.3390/SU13169463
- [12] Azroul M, Mabrouki J, Guezzaz A, Kanwal A. Internet of Things security: Challenges and key issues. *Security and Communication Networks*. 2021;**2021**. DOI: 10.1155/2021/5533843
- [13] Dorsemaine B, Gaulier JP, Wary JP, Kheir N, Urien P. A new approach to investigate IoT threats based on a four layer model. In: 13th International Conference on New Technologies for Distributed Systems (NOTERE 2016). IEEE; 2016. DOI: 10.1109/NOTERE.2016.7745830
- [14] Russell S, Peter N. *Artificial intelligence: a modern approach*. Harvard: Prentice Hall; 2010

- [15] Negnevitsky M. *Artificial Intelligence: A Guide to Intelligent Systems*. 3rd ed. Addison Wesley/Pearson; 2011
- [16] Lantz B. *Machine Learning with R: Expert Techniques for Predictive*. Birmingham, UK: Packt Publishing Ltd; 2019
- [17] Moustafa M, Choo KKR, Abu-Mahfouz AM, Guest editorial: AI-enabled threat intelligence and hunting microservices for distributed industrial IoT system. *IEEE Transactions on Industrial Informatics*. 2022;**18**(3). Available from: <https://ieeexplore.ieee.org/document/9536391/> [Accessed: February 7, 2022]
- [18] Gebremichael T et al. Security and privacy in the industrial Internet of Things: Current standards and future challenges. *IEEE Access*. 2020;**8**: 152351-152366. DOI: 10.1109/ACCESS.2020.3016937
- [19] Chui M, Collins M, Patel M. McKinsey Report: The Internet of Things Catching up to an Accelerating Opportunity. Fluxus; 2021. Available from: <https://fluxus-prefab.com/mckinsey-report-the-internet-of-things-catching-up-to-an-accelerating-opportunity/>. [Accessed: February 11, 2022]
- [20] Osterwalder A, Pigneur Y. *Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers* (The Strategyzer Series). John Wiley and Sons; 2010
- [21] Dijkman RM, Sprenkels B, Peeters T, Janssen A. Business models for the Internet of Things. *International Journal of Information Management*. 2015;**35**(6): 672-678. DOI: 10.1016/J.IJINFOMGT.2015.07.008
- [22] Cranmer EE, Papalexi M, tom Dieck MC, Bamford D. Internet of Things: Aspiration, implementation and contribution. *Journal of Business Research*. 2022;**139**:69-80. DOI: 10.1016/J.JBUSRES.2021.09.025
- [23] Suppatvech C, Godsell J, Day S. The roles of Internet of Things technology in enabling servitized business models: A systematic literature review. *Industrial Marketing Management*. 2019;**82**:70-86. DOI: 10.1016/J.INDMARMAN.2019.02.016
- [24] Mansour H, Presser M, Bjerrum T. Comparison of seven business model innovation tools for IoT ecosystems. *IEEE World Forum Internet Things*. 2018;**2018**:68-73. DOI: 10.1109/WF-IOT.2018.8355219
- [25] Manyika J, Chui M, Bisson P, Woetzel J, Dobbs R. *The Internet of Things: Mapping the Value beyond the Hype*. McKinsey Global Institute; 2015
- [26] George G, Thampi SM. A graph-based security framework for securing industrial IoT networks from vulnerability exploitations. *IEEE Access*. 2018;**6**:43586-43601. DOI: 10.1109/ACCESS.2018.2863244
- [27] Fang L, Zhang H, Li M, Ge C, Liu L, Liu Z. A secure and fine-grained scheme for data security in industrial IoT platforms for smart city. *IEEE Internet Things Journal*. 2020;**7**(9). Available from: <https://ieeexplore.ieee.org/document/9104725/>. [Accessed: February 6, 2022]
- [28] Tariq U, Aseeri AO, Alkathairi MS, Zhuang Y. Context-aware autonomous security assertion for industrial IoT. *IEEE Access*. 2020;**8**:191785-191794. DOI: 10.1109/ACCESS.2020.3032436
- [29] Rathore S, Park JH, Chang H. Deep learning and blockchain-empowered security framework for intelligent 5G-

enabled IoT. IEEE Access. 2021;**9**: 90075-90083. DOI: 10.1109/ACCESS.2021.3077069

[30] El Kaed C, Khan I, Van Den Berg A, Hossayni H, Saint-Marcel C. SRE: Semantic rules engine for the industrial Internet-of-things gateways, IEEE Transactions on Industrial Informatics. 2018;**14**(2). Available from: <https://ieeexplore.ieee.org/document/8091285/>. [Accessed: February 7, 2022]

[31] Iwendi C, Rehman SU, Javed AR, Khan S, Srivastava G. Sustainable security for the Internet of Things using artificial intelligence architectures. ACM Transactions on Internet Technology. 2021;**21**(3):73. DOI: 10.1145/3448614

[32] Microsoft, IoT Security Architecture Microsoft Docs. 2021. Available from: <https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-architecture>. [Accessed: February 11, 2022]

[33] Sven Schrecker H. Industrial Internet of Things volume G4: Security Framework. Industrial Internet Consortium. 2016

[34] Microsoft. Azure IoT Reference Architecture. Microsoft; 2021. Available from: <https://azure.microsoft.com/en-us/resources/microsoft-azure-iot-reference-architecture/>. [Accessed: February 12, 2022]

[35] Aufner P. The IoT security gap: A look down into the valley between threat models and their implementation. International Journal of Information Security. 2020;**19**(1):3-14. DOI: 10.1007/S10207-019-00445-Y/FIGURES/1

[36] Flauzac O, Gonzalez C, Nolot F. New security architecture for IoT network. Procedia Computer Science. 2015;**52**(1): 1028-1033. DOI: 10.1016/J.PROCS.2015.05.099

[37] ENISA, Baseline Security Recommendations for IoT — ENISA. 2017.

[38] Alshohoumi F, Sarrab M, AlHamadani A, Al-Abri D. Systematic review of existing IoT architectures security and privacy issues and concerns. International Journal of Advanced Computer Science and Applications. 2019;**10**(7):232-251. DOI: 10.14569/IJACSA.2019.0100733

[39] OWASP. OWASP IoT Security Verification Standard OWASP Foundation. OWASP; 2022. Available from: <https://owasp.org/www-project-iot-security-verification-standard/>. [Accessed: February 12, 2022]

[40] Zhang J, Jin H, Gong L, Cao J, Gu Z. Overview of IoT security architecture. In: 2019 IEEE 4th International Conference on Data Science in Cyberspace, DSC. 2019. pp. 338-345. DOI: 10.1109/DSC.2019.00058

[41] Sharma N, Prakash R, Rajesh E. Different dimensions of IOT security. International Journal of Recent Technology and Engineering. 2020;**8**(5): 2277-3878. DOI: 10.35940/ijrte.E5893.018520

[42] Ahanger TA, Aljumah A. Internet of Things: A comprehensive study of security issues and defense mechanisms. IEEE Access. 2019;**7**:11020-11028. DOI: 10.1109/ACCESS.2018.2876939

[43] Litoussi M, Kannouf N, El Makkaoui K, Ezzati A, Fartitchou M. IoT security: Challenges and countermeasures. Procedia Computer Science. 2020;**177**:503-508. DOI: 10.1016/J.PROCS.2020.10.069

[44] Ávila K, Sanmartin P, Jabba D, Gómez J. An analytical survey of attack scenario parameters on the techniques of attack mitigation in WSN. Wireless

Personal Communications. 2022;**122**(4): 3687-3718. DOI: 10.1007/S11277-021-09107-6/FIGURES/19

[45] Restuccia F, D'Oro S, Melodia T. Securing the Internet of Things in the age of machine learning and software-defined networking. *IEEE Internet of Things Journal*. 2018;**5**(6):4829-4842. DOI: 10.1109/JIOT.2018.2846040

[46] Hassija V, Chamola V, Saxena V, Jain D, Goyal P, Sikdar B. A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access*. 2019;**7**:82721-82743. DOI: 10.1109/ACCESS.2019.2924045

[47] Noor MM, Hassan WH. Current research on Internet of Things (IoT) security: A survey. *Computer Networks*. 2019;**148**:283-294. DOI: 10.1016/J.COMNET.2018.11.025

[48] Miller D. Blockchain and the Internet of Things in the industrial sector. *IT Professional*. 2018;**20**(3):15-18. DOI: 10.1109/MITP.2018.032501742

[49] Giotis K, Argyropoulos C, Androulidakis G, Kalogeras D, Maglaris V. Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments. *Computer Networks*. 2014;**62**:122-136. DOI: 10.1016/J.BJP.2013.10.014

[50] Wu H, Han H, Wang X, Sun S. Research on artificial intelligence enhancing Internet of Things security: A survey. *IEEE Access*. 2020;**8**: 153826-153848. DOI: 10.1109/ACCESS.2020.3018170

[51] Puthal D, Mishra A, Sharma S. AI-driven security solutions for the internet of everything. *IEEE Consumer Electronics Magazine*. 2021;**10**(5):70-71. DOI: 10.1109/MCE.2021.3071676

[52] Bagaa M, Taleb T, Bernabe JB, et al. A machine learning security framework for IoT systems. *IEEE Access*. 2020;**8**: 114066-114077. Available from: <https://ieeexplore.ieee.org/abstract/document/9097876/>. [Accessed: February 04, 2022]

[53] Kuzlu M. Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. *Discover Internet of Things*. 2021;**1**(1):1-14. DOI: 10.1007/S43926-020-00001-4

[54] Liu M, Xue Z, He X. Two-tier intrusion detection framework for embedded systems. *IEEE Consumer Electronics Magazine*. 2021;**10**(5):102-108. DOI: 10.1109/MCE.2020.3048314

[55] Zaman S et al. Security threats and artificial intelligence based countermeasures for Internet of Things networks: A comprehensive survey. *IEEE Access*. 2021;**9**:94668-94690. Available from: <https://ieeexplore-ieee-org.masader.idm.oclc.org/document/9456954/>. [Accessed: February 05, 2022]

[56] Jayalaxmi P, Saha R, Kumar G, Kumar N, Kim TH. A taxonomy of security issues in industrial Internet-of-Things: Scoping review for existing solutions, future implications, and research challenges. *IEEE Access*. 2021;**9**: 25344-25359. DOI: 10.1109/ACCESS.2021.3057766

[57] Aboelwafa MMN, Seddik KG, Eldefrawy MH, Gadallah Y, Gidlund M. A machine-learning-based technique for false data injection attacks detection in industrial IoT. *IEEE Internet of Things Journal*. 2020;**7**(9). Available from: <https://ieeexplore-ieee-org.masader.idm.oclc.org/document/9084134/>. [Accessed: February 11, 2022]

[58] Hassan MM, Gumaei A, Huda S, Almogren A. Increasing the trustworthiness in the industrial IoT

networks through a reliable cyberattack detection model. *IEEE Transactions on Industrial Informatics*. 2020;**16**(9). Available from: <https://ieeexplore-ieee-org.masader.idm.oclc.org/document/8972480/>. [Accessed: February 11, 2022]

IntechOpen

IntechOpen