

IoT Security, Privacy, Safety and Ethics



Hany F. Atlam and Gary B. Wills

Abstract The Internet of Things (IoT) represents a revolution of the Internet which can connect nearly all environment devices over the Internet to share their data to create novel services and applications for improving our quality of life. Using cheap sensors, the IoT enables various devices and objects around us to be addressable, recognizable and locatable. Although the IoT brought infinite benefits, it creates several challenges, especially in security and privacy. Handling these issues and ensuring security and privacy for IoT products and services must be a fundamental priority. Users need to trust IoT devices and related services are secure. Moreover, the IoT safety must be considered to prevent the IoT system and its components from causing an unacceptable risk of injury or physical damage and at the same time considering social behaviour and ethical use of IoT technologies to enable effective security and safety. This chapter provides a discussion of IoT security, privacy, safety and ethics. It starts by providing an overview of the IoT system, its architecture and essential characteristics. This is followed by discussing IoT security challenges, requirements and best practices to protect IoT devices. The IoT privacy is also discussed by highlighting various IoT privacy threats and solutions to preserve the privacy of IoT devices. The IoT safety, ethics, the need for the ethical design and challenges encountered are also discussed. In the end, smart cities are introduced as a case study to investigate various security threats and suggested solutions to maintain a good security level in a smart city.

Keywords Internet of things · IoT security and privacy · Ethical design for IoT · IoT safety · Security by design · Privacy by design

H. F. Atlam (✉) · G. B. Wills

School of Electronics and Computer Science, University of Southampton, Southampton, UK
e-mail: hfa1g15@soton.ac.uk

G. B. Wills

e-mail: gbw@soton.ac.uk

H. F. Atlam

Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Menoufia, Egypt

© Springer Nature Switzerland AG 2020

M. Farsi et al. (eds.), *Digital Twin Technologies and Smart Cities*,
Internet of Things, https://doi.org/10.1007/978-3-030-18732-3_8

1 Introduction

Currently, the Internet of Things (IoT) has become one of the hottest topics among researchers and experts. It is considered a universal presence that allows all objects/things in our environment to be connected over the Internet with the capability to interconnect with each other without human intervention. The IoT involves a variety of objects that can be connected using either wireless or wired networks. These objects have a unique addressing scheme that allows them to interact and cooperate with each other to create novel applications and services such as smart homes, smart transportation, connected cars, smart grids, smart cities, smart traffic control and others [1].

The social acceptance of IoT applications and services is strongly depending on the trustworthiness of information and the protection of private data. Since the IoT is a complex, distributed and heterogeneous system in nature, it faces several challenges regarding security and privacy. Currently, building an effective and reliable security technique is one of the highest priorities to consider [2]. Although a number of researchers have introduced several solutions to the security and privacy issues, a reliable security technique for the IoT is still in demand to satisfy requirements of data confidentiality, integrity, privacy and trust [3].

In addition, the IoT safety is considered to be one of the highest significances to prevent the IoT and its elements from producing physical damage or undesirable threat and protect the surrounding environment from such damage. Building the IoT system with embedded safety and reliability features should be considered to create new design architectures that provide a safe and reliable system environment [4]. In addition, there is a need to develop an ethical framework that ensures the IoT is used for the good of humanity and not the other way around. A strong ethical standard will motivate companies to design smarter and more inclusively products to avoid algorithmic issues and ensure global connectivity.

The main objective of this chapter is to provide an overview of IoT security, privacy, safety and ethics. It starts by discussing the architecture and essential characteristics of the IoT system. This is followed by investigating IoT security by highlighting security requirements, security by design, security attacks and security challenges of the IoT system. IoT privacy with investigating privacy threats and suggested solutions are also discussed. Also, IoT safety and ethics are investigated by highlighting the need for ethical design and ethics challenges in the IoT system. In the end, a case study of the smart city is introduced to discuss security threats and suggested solutions in the smart city context.

The rest of this chapter is structured as follows: Sect. 2 provides an overview of the IoT system; Sect. 3 discusses IoT security; Privacy issues and suggested solutions are discussed in Sect. 4; Sect. 5 discusses IoT safety; the need for ethical design and ethics challenges in the IoT are presented in Sect. 6; Sect. 7 discusses security issues and suggested solution in the smart city context; Sect. 8 is the conclusion.

2 An Overview of IoT

This section provides an overview of the IoT system by discussing IoT definitions, its layer architecture and essential characteristics.

2.1 IoT Definition

The IoT system has evolved to involve the perception of realizing a global infrastructure of interconnected networks of physical and virtual objects. These objects/things are interconnected using either wired or wireless networks to share information between various IoT devices to create novel applications and services [5].

Originally, the notion of the IoT was initially presented by Kevin Ashton, who is the originator of MIT auto-identification centre in 1999 [6]. Ashton has said, *‘The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so’* [6]. Later, the IoT was officially presented by the International Telecommunication Union (ITU) in 2005 [7]. The IoT has been defined by many organizations and researchers. However, the definition provided by ITU in 2012 is the most common. It stated: *‘a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies’* [8].

In addition, Guillemin and Friess [9] have suggested one of the simplest definitions that describe the IoT in a smooth manner, as shown in Fig. 1. It stated: *‘The Internet of Things allows people and things to be connected Anytime, Anyplace, with anything and anyone, ideally using any path/network and any service’*. Several definitions were suggested by many researchers describing the IoT system from different perspectives but the important thing that majority of researchers have agreed on the IoT is created to increase information sharing that leads to a better world for all the human beings.

2.2 IoT Essential Characteristics

The IoT represents a promising technology that aims to improve people’s quality of life by generating new applications that facilitate people daily activities. For the IoT system, there are a set of common features, which include the following:

- **Large Scale:** IoT devices are increased in billions. This large-scale network of devices needs to be controlled to allow devices to communicate with each other. In addition, this large-scale network generates a huge amount of data which produce a critical issue regarding data interpretation and analysis.
- **Intelligence:** Combining sophisticated software algorithms with hardware allow IoT devices to become smart. These intelligence abilities allow IoT devices to

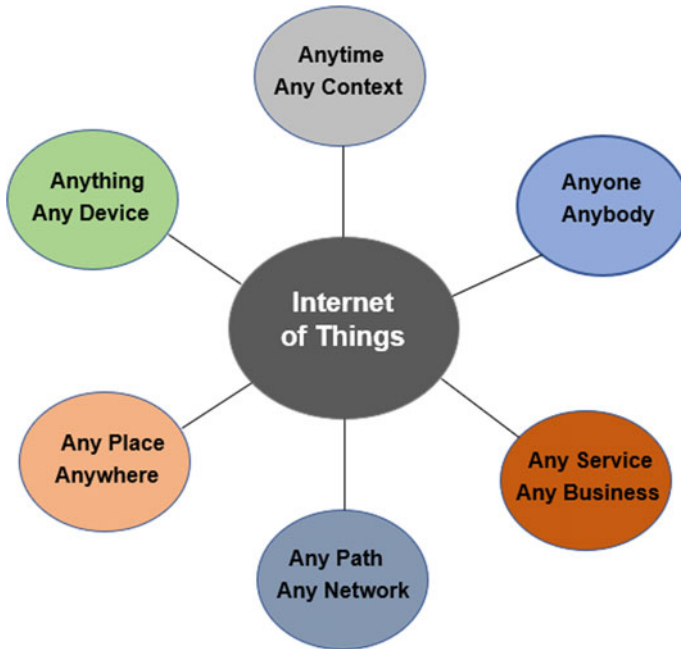


Fig. 1 The IoT can connect anything anywhere using any path

make intelligent decisions in various situations and interact intelligently with other communicating devices.

- **Sensing:** Sensors are the main part of the IoT system which are used to perceive changes in the surrounding environment and create data that reveal their status. With various sensing technologies, sensors provide a good understating of surroundings and increase human awareness about the physical world [8].
- **Complex System:** The IoT system consists of billions of heterogamous objects with different hardware and software capabilities that make the management process a very difficult task to accomplish especially with constraints associated with memory, energy and time.
- **Dynamic Environment:** The IoT has the ability to connect almost all objects of our environment without having to determine the IoT network boundaries which make it a dynamic system in nature. Also, IoT devices can operate and be adjusted dynamically based on changing conditions and situations.
- **Massive Amount of Data:** As IoT devices are in billions. These devices sense their surroundings and generate a huge amount of data which make it one of the sources of what is called Big Data.
- **Heterogeneity:** The IoT system involves billions of devices with heterogeneous features such as operating systems, platforms, communication protocols and others. These heterogeneous features make the management operation a complex task to perform.

- **Limited Energy:** Most IoT devices are small and lightweight with limited resources, so they are designed to work with minimal energy consumption.
- **Connectivity:** One of the main features of the IoT system is the ability to connect various devices with different characteristics and use their shared information to create novel applications and services.
- **Self-configuring:** Devices are configured to perform a certain operation. But for IoT devices, they have the capability of self-configuring that enable them to operate without human intervention. IoT devices could configure themselves to the up-to-date software in association with the device manufacturer without user involvement.
- **Unique Identity:** Within the IoT network, each IoT object is identified and recognized using a unique identifier such as the IP address. These identities are provided by IoT manufactures to use it to upgrade devices to the appropriate platforms. In addition, these devices have interfaces that enable users to collect the required information from the devices, record their status and manage them remotely.
- **Context awareness:** In the IoT environment, there are multiple sensors that sense their surroundings, collect and store the required information, these sensors may take decisions based on collected data which make it a context aware.

2.3 *IoT Architecture*

IoT World Forum (IWF) architecture committee released an IoT reference model in October 2014 [10]. This model works as a common framework to help the industry to accelerate IoT deployments. This reference model is intended to consolidate and encourage the collaboration and development of IoT deployment models. It is designed as seven layers so that each layer provides additional information for establishing a common terminology, as shown in Fig. 2. It also classifies where various kinds of processing are operated through different layers of the IoT reference model. In addition, this model enables various manufacturers to produce IoT products that are compatible with each other, which convert the IoT from a conceptual model into a real and approachable system. Layer 1 is the physical layer. It contains physical devices and controllers that manage various objects. These objects represent things in the IoT that involve various types of devices that send and receive information, for instance, sensors that collect information about the surrounding environment [11]. Communications and connectivity are in layer 2. This layer is used to interconnect different IoT things with each other using interconnection devices such as switches, gateway, router and firewalls. Layer 3 is edge computing. This layer takes data coming from the connectivity layer and converts it into information appropriate for storage and higher level processing. At this layer, the processing components work with a huge amount of data and it may execute some data transformation to reduce the size of data. Layer 4 is the data accumulation. This layer is concerned with storing data coming from different IoT devices. This data is filtered and processed by the edge-computing layer that absorbs large quantities of data and places them in

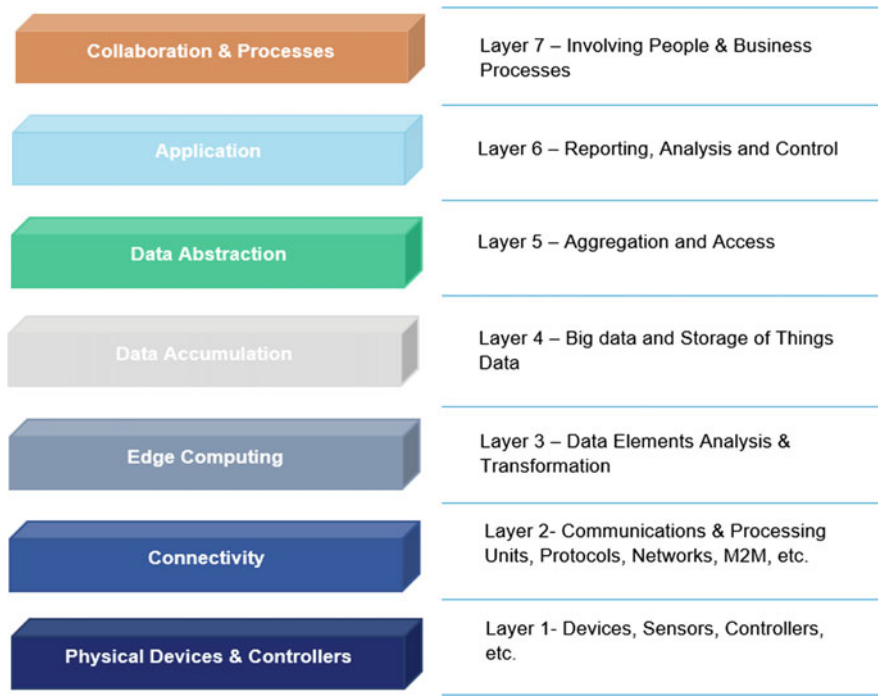


Fig. 2 The IoT reference model according to IWF, drawn from data provided in [13]

storage to be accessible by higher levels. Different types of data in various formats and from heterogeneous processors may come up from the edge-computing layer for storage. The data abstraction layer aggregates and formats stored data in a way that make them accessible by applications in a more manageable and efficient way. Layer 6 is the application layer. This layer is concerned with the information interpretation of various IoT applications. This layer encompasses a variety of applications that use IoT input data or control IoT devices [10]. The collaboration and processes are in layer 7. This layer identifies individuals who can communicate and collaborate to make the IoT system more useful. It also involves various applications to exchange data and control information over the Internet.

3 IoT Security

Majority of researchers and experts have confirmed that securing the IoT system is one of the most serious challenges that stand in the way of successful adoption of IoT devices. The value of the IoT system comes from connecting all small and

large systems together and allowing them to communicate with each other over the Internet.

Since the IoT is a dynamic system in nature in which every poorly secured object can disturb the security and resilience of the entire system as they are connected like a chain. The ease of connection and access of IoT devices open doors for severe security issues especially with the large-scale distribution of heterogamous devices, their ability to connect to other devices without requesting permissions or even notifying their owners and probability of flooding these devices with severe security threats [12].

Handling security challenges in the IoT context should be a fundamental priority to increase adoption of IoT applications. Users need to be fully confident about the security of their IoT devices and related applications. They need to ensure that their devices are totally secured from various known threats as they become more integrated into people daily life's activities [13].

3.1 Security Requirements for IoT

Security of the IoT system can be assessed by employing classical security and risk analysis measures [14]. Typical CIA (Confidentiality, Integrity and Availability) security requirements should be employed in the IoT system.

Confidentiality means exchanging messages between a sender and receiver should be protected against any malicious or unauthenticated user [15]. For the IoT system, confidentiality need not only to be guaranteed inside the communication network but also when transmitting messages between various IoT devices. Integrity is used to guarantee the content of messages exchanged between the sender and receiver which is protected against any manipulation by an intruder without the receiver being able to track this manipulation. In the IoT system, the integrity check can be carried out at each node involved in the message exchange between the sender and receiver. Availability is used to guarantee that a malicious user is not capable of disrupting or harmfully affecting communication or quality of service provided by IoT devices or communication network [16].

Although CIA is essential for the IoT, there are other security requirements that are needed to be implemented for each level of the IoT architecture, as shown in Fig. 3. Node authentication is the main security issue for the physical layer to avoid unauthenticated node access and keep the communication channel between IoT nodes safe from any type of attack. Lightweight cryptographic algorithm and protocol is an important aspect to encrypt transmitted data especially for resources-constrained IoT devices [17].

For the connectivity or network layer, communication security measures are needed as well as identity authentication to prevent illegal nodes. Also, Distributed Denial of Service (DDoS) attack is common at this level, so there is a need to protect against DDOS attack in defenceless nodes in this layer, especially it is more severe in the IoT context [18]. For data abstraction, accumulation and edge-computing level,

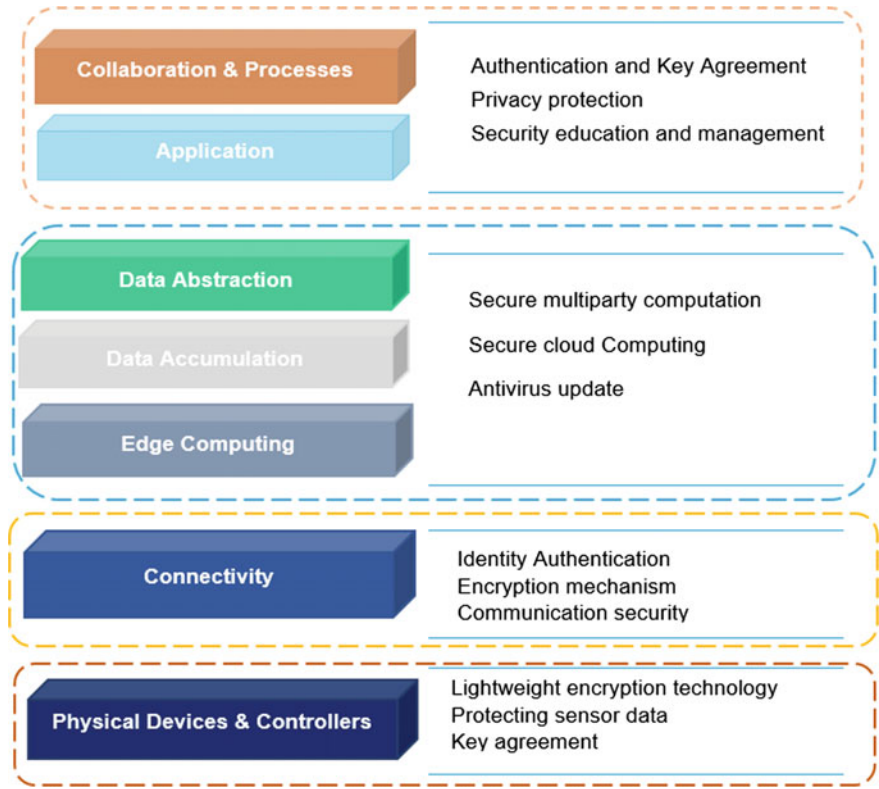


Fig. 3 Security requirements at each level of the IoT architecture

many application security mechanisms are needed to secure data stored in cloud computing. Strong encryption algorithms are needed besides an updated antivirus. While for the application and collaboration level, there is a need to adopt authentication and key agreement to protect user’s privacy. Moreover, education and password management are essential for information security at this level [17].

3.2 Security by Design for IoT

Security by design is a novel approach suggested by several organizations to implement required security measures in the software and hardware development life cycle and not after detecting a security breach. The necessity to adopt security by design becomes essential to protect billions of IoT devices that are poorly secured against common security attacks. Since these devices are connected to the Internet, they become a weak point that can be exploited by any security attacker to steal sen-

sitive information or disrupt the service. Also, the majority of these devices were built without security built into their system, making them easy targets for security attackers [1].

Security by design aims to protect the security of devices by the manufacturers. The user awareness of security has proved that it creates many vulnerabilities and threats that can affect people lives. Security by design can help the user to understand IoT security requirements and encourages them to make the right decisions to ensure their security and safety [19].

The UK government demand security by design in new products to address IoT security. The government argued that companies should integrate sufficient security mechanisms into their IoT devices to protect them from potential threats [20]. The government is also looking into providing incentives for the IoT industry to promote security by design for vendors and provide more information about built-in device security for consumers at purchase. Their strategy includes encouraging companies and developers to build safety features into their products from the beginning, to ensure connected devices are secure in both the design phase and throughout the life cycle of various products.

3.3 Best Practice for Securing IoT Devices

Security concerns associated with IoT devices create potential risks in our life. Before the IoT, a security breach can lead to losing your money, but with IoT, security attack can literally result in losing your life. Securing IoT devices requires taking a set of best practices that include the following:

- **Hardware Tamper Resistant:** Keeping IoT devices isolated and only certain people have physical access to it are the major steps to make your IoT devices tamper proof or tamper evident. Also, IoT device hardening with physical security such as blocking unused ports and covering camera are good points to prevent potential attackers from reaching your data [21].
- **Strong Authentication:** Many IoT users still use weak and default passwords without any update. Manufacturers should ask the customer to update the default one with strong passwords before using the device. In addition, alternative ways to recognize devices identity and trust are needed since username and password are not realistic for every device, especially for Machine-to-Machine (M2M) communication which starts to grow significantly [22].
- **Firmware Updates:** IoT devices must be patchable or upgradable with a proper digital signature. There are several serious threats on the Internet that affect IoT devices. Vendors and service providers should plan for future upgrades of devices' software to keep it up to date. These updates required to be accomplished on a time basis or subject to the importance of the update [23].
- **Device Identity Spoofing:** The sending and receiving nodes should be identified as legitimate devices. Therefore, it is significant to secure against IoT device identity

spoofing since setting and handling unique identities have been difficult for IoT devices due to their small and lightweight size.

- **Dynamic Testing:** It is critical for IoT devices to go through testing and create the least standard measures for security. To test the security of IoT devices, there are two types; static and dynamic. In contrast to static testing that is concerned with discovering threats in software, dynamic testing can explore threats and vulnerabilities in both hardware and software [21].
- **Failover Design:** IoT devices should operate appropriately in the case of losing or disrupting Internet connectivity. However, few IoT devices are built to work with such failure situations such as the Internet continuity or data disconnections. Failover design is essential for IoT devices that include user safety, such as door lock mechanisms, video monitoring, and environmental monitors and alarms. These devices should have additional features in the case of disconnected operations [24].

3.4 *IoT Security Attacks*

The IoT system with distributed and dynamic nature creates weak communication channels which are used by malicious objects to exploit and open new threats regarding tracking, monitoring and reporting of the users' actions. The increase of IoT devices in our community has presented a set of security attacks that need to be addressed. There are four main types of attacks in the IoT system, physical, software, network and encryption attacks. This section provides a brief discussion of each type of attack and its common examples within IoT systems. Various security attacks in the IoT system are summarized in Fig. 4.

3.4.1 **Physical Attacks**

These types of attacks are concerned with the hardware elements of the IoT system in which the attacker requires to be physically near to the IoT system to run the attack. These attacks are relatively difficult to achieve because they require expensive substances [25]. Physical attacks can have different forms which include the following:

- **Node Tampering:** This attack targets the sensor node by physically damaging it or even replaces the entire node or part of its hardware to gain the access to sensitive information [26].
- **RF Interference on RFIDs:** This attack targets the availability of the IoT sensors. The attacker uses Radio Frequency Identification (RFID) tag to direct noise signals using the Radio Frequency (RF) signals used by RFIDs for communication. These signals interfere with RFID signals which affect the quality of communication [27].

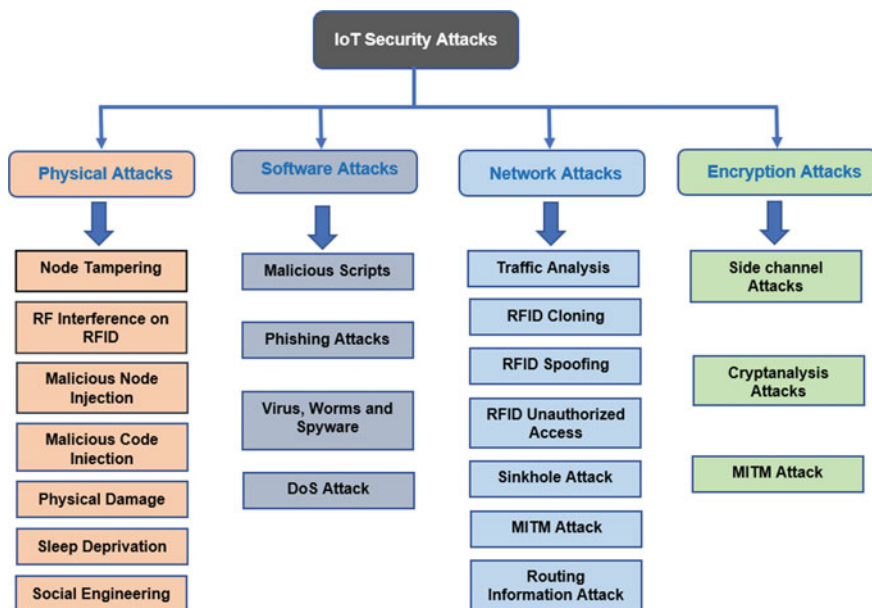


Fig. 4 Various security attacks in the IoT system

- **Malicious Node Injection:** The attacker gains the access to sensitive information by physically operating a new malicious node between communicating nodes of the IoT system, which allows the attacker to control all data flow between various nodes.
- **Malicious Code Injection:** This type of attack focuses on physically injecting the IoT node with malicious code that helps to gain access to the IoT system.
- **Physical Damage:** This type of attack is similar to node tampering in which the attacker physically damages IoT devices. This type of attack is difficult to achieve as it requires the attacker to reach area or building containing IoT devices to destroy it. The major difference between this attack and node tampering attack is that the attacker attempts to harm the IoT system directly to affect system availability and quality of service [26].
- **Sleep Deprivation:** Most sensors are operated through useable batteries that work according to sleep routine to enlarge their battery life. The sleep deprivation attack retains the nodes running at all times which leads to more energy feasting that results in shutting down of nodes after consuming battery energy [26].
- **Social Engineering:** The attacker uses the lack of security awareness of users to manipulate and gain access to the IoT system to collect sensitive information or to accomplish particular activities to serve his goals.

3.4.2 Software Attacks

Software attacks are the main cause of most security threats in almost all software systems. They target the weaknesses and threats found in the system implementation using its communication interfaces [25]. There are a set of software attacks which include the following:

- **Malicious Scripts:** Since the IoT system is linked to the Internet, the attacker uses this facility to create malicious scripts that aim to gain access to sensitive data or disturb system availability. These malicious scripts are executed through system users by wrong [28].
- **Phishing Attacks:** It is a kind of social engineering attack which targets user login credentials and other sensitive information through infected emails or phishing websites.
- **Virus, Worms and Spyware:** This type of attack is closed to malicious code injection attack in which the attacker injects the system with malicious software to gain access to the system, steal sensitive information or disrupt system availability [28].
- **DoS Attack:** An attacker can perform Denial of Service (DoS) on the IoT system across the application layer which affects all users of the IoT network. This type of attack also blocks legal users and gives the attacker the full access to sensitive data [25].

3.4.3 Network Attacks

The IoT system is a combination of networks interconnected together to transfer data between various IoT devices. Network attacks are concerned with the IoT network in which the attacker does not essentially require to be near to the network for the attack to operate. There are a set of network attacks which include the following:

- **Traffic Analysis Attacks:** This type of attack is concerned with sniffing out sensitive data and other types of data due to their wireless features. Moreover, in most attacks, it is necessary for the attacker to collect some network information before operating any attacks, and this is achieved by using a traffic analysis attack [29].
- **RFID Spoofing:** This type of attack is concerned with spoofing RFID signals to obtain data stored on an RFID tag. Then, the attacker uses the original tag ID to send his own data to appear to be from the original source, which enables the attacker to access the entire system as a legal node [30].
- **RFID Cloning:** This type of attack targets RFID tag by copying its own data to another RFID tag. Although the two RFID tags have identical data, it does not duplicate the original ID of the RFID [30].
- **RFID Unauthorized Access:** Due to the lack of appropriate authentication techniques in most RFID nodes, it is easy to be hacked by anyone allowing the intruder to read, edit or even delete data on RFID nodes.

- **Sinkhole Attack:** This type of attack targets the confidentiality of data and disrupt network service by discarding all packets instead of forwarding them to the desired destination [31].
- **MITM Attack:** Man-In-The-Middle (MITM) attack is operated by placing a malicious node between two communicating nodes which allow it to intercept and monitor all traffic sent between communicating nodes. Depending on the network communication protocols of the IoT system, the attacker does not need to be physically close to the network to run the attack [32].
- **Routing Information Attacks:** Routing table information is used by the network router to forward data to their desired destinations. Hence, this type of attack targets this table by spoofing or changing its contents which disrupt network service and most traffic will be discarded and error messages will be sent [30].

3.4.4 Encryption Attacks

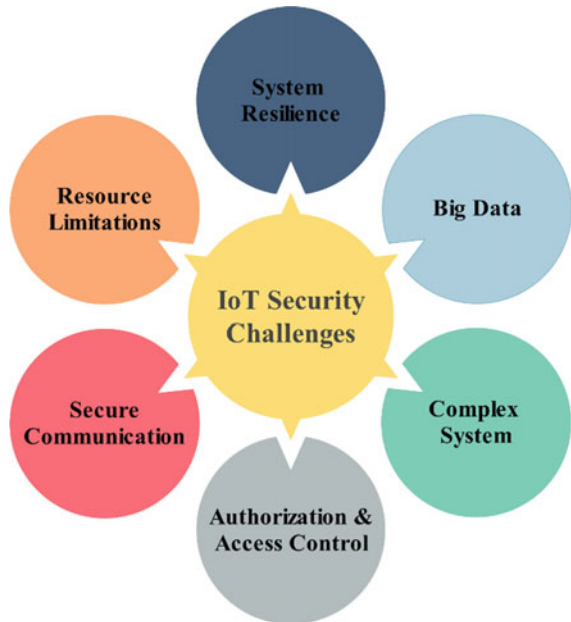
The IoT system connects all objects through various communication channels. To protect the communication process, encryption algorithms are used. However, nothing is unbreakable. Encryption attacks are focused on breaching the encryption structure used in the IoT system [26]. There are a set of encryption attacks which include the following:

- **Side Channel Attacks:** This attack targets encryption devices in the IoT system using certain techniques to reach encryption and decryption keys used in the data encryption process.
- **Cryptanalysis Attacks:** If we suppose that the attacker already has the ciphertext or plaintext, then the attacker's goal becomes to find the encryption key by breaking the system encryption structure. There are several forms of cryptanalysis attacks such as chosen ciphertext, known-plaintext, ciphertext-only and chosen-plaintext attack [26].
- **MITM Attack:** For two nodes to communicate with each other on a secure communication channel using an encryption algorithm, they exchange encryption and decryption key. MITM attack tries to gain the access to this information by intercepting signals sent between two nodes and tries to execute a key exchange with each node separately, which enables the attacker to encrypt and decrypt any future signals between communicating nodes [32].

3.5 IoT Security Challenges

Like all new technologies, security issues are still the biggest problems that stand in the path of effective developments of the IoT system. There are several security challenges that need to be addressed to increase people trust in adopting IoT devices.

Fig. 5 Security challenges of the IoT system



This section provides a brief discussion of common security challenges in the IoT system, as summarized in Fig. 5.

3.5.1 Resource Limitations

Most IoT devices have limited processing and storage capabilities, due to small and lightweight features which make them run on lower energy. Therefore, sophisticated security algorithms are not suitable for these constrained devices as they are not able to execute complex processing operations in real time. Instead, constrained devices typically only employ fast, lightweight encryption algorithms [33].

3.5.2 Big Data

As said earlier, the IoT system involves billions of devices which generate a huge amount of data. These data are variable in terms of structure and often arrive in real time. The volume, velocity and variety make storing and analysis process, which is used to generate meaningful information, a very complex task. The IoT is one of the main sources of big data. Using cloud computing can facilitate storing this huge amount of data for a long period of time. However, handling this massive data is a substantial challenge, as the entire performance of various applications is significantly dependent on the data management service. Moreover, one of the

essential aspects of big data is data integrity. Ensuring the security of this huge amount of data is becoming difficult as data sources massively increased in a way that more security measures need to be adopted [34].

3.5.3 Authorization and Access Control

Providing an efficient authorization and access control mechanism for the IoT system is one of the major fundamentals to provide a secure system. IoT devices should gain access to services or applications only after providing their identities correctly. However, there are many problems associated with device authentication such as the use of weak or default passwords that lead to giving access to attackers who can manipulate device data or even physically damage it. Adopting security by design in IoT devices, enabling two-factor authentications and enforcing the use of strong passwords can help to address these challenges [35].

3.5.4 Secure Communication

Securing the IoT devices is not enough to ensure that the full security has been achieved in the IoT system. Instead, the communication channel connecting various communicating nodes such as IoT devices and cloud services needs to be protected from any attack. Most IoT devices send data in the plaintext format without encryption which make it an easy target to various types of network attacks. Hence, a proper encryption technique should be employed. Also, using separate networks can increase security through isolating devices and creating private communication channels.

3.5.5 System Resilience

Resilience is one of the main challenges that need to be addressed in the IoT system. System resilience refers to the ability of the system to respond to unpredicted attacks/situations without regressing. Hence, if some IoT devices are hacked, the system should be able to protect other network nodes from any attack.

3.5.6 Complex System

The IoT system involves billions of heterogeneous devices which make the management of this large-scale network a very difficult task to accomplish, especially with constraints associated with memory, energy and time. The more devices, people, interactions and interfaces, the more the risk of security breaches. In other words, with more variety and diversity in the IoT system, the challenges of managing all points in the network to maximize security become a difficult operation to achieve [2].

4 IoT Privacy

The IoT growth continues to add billions of new sensors and devices to the Internet, generating an enormous amount of information about people, including their locations, connections, shopping records, financial transactions, pictures, voices, conversations, health state, etc., with or without their consent. This huge amount of information makes retaining our privacy a difficult task [36].

The privacy in the IoT system can take many forms, but first, we need to define what privacy means. According to Westin [37], the privacy is defined as ‘*The claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others*’.

Privacy is a notion that is associated with four main elements: information, communications, body and territory. Information privacy is related to various types of personal data collected and processed by an organization, such as financial and medical information, while the privacy of communication is concerned with protecting data sent between two communicating nodes using any communication medium. Body privacy is concerned with people’s physical safety alongside any outside damage, whereas territorial privacy is concerned with building limits on physical space such as home, workplace and public places [38].

In the IoT context, protecting people privacy has become a very difficult task to achieve. This is because the data collection process is more passive, pervasive and less intrusive, which leads to making users less aware of being tracked. The potential risk of losing control over personal information is defined as a privacy threat. This threat is usually one of the key concerns of users and has an important effect on the adoption level of any new technology [39].

4.1 IoT Privacy Threats

One of the important characteristics of the IoT is the capability of objects to perceive and sense their environment. But this capability leads to tracking and monitoring user actions and activities which violate user privacy and results in many problems that can literally lead to losing people lives. This section provides a discussion of common privacy threats in the IoT system.

4.1.1 Identification

The IoT system is pervasive in nature that allows devices to sense and collect various types of data about users and their interactions with the environment. Typically, these data are processed at service providers, which are located outside of users’ control.

Identification is the threat of relating an identifier (e.g., name, address) with private data about an individual. In the IoT, new technologies and interconnection of

various techniques expand the threat of identification [40]. The use of a surveillance camera, in non-security contexts, is an example of such techniques, where customers' behaviour is studied for analysis and marketing. To address this issue, attribute-based authentication is recommended to minimize the data a device can collect in the IoT and maintain control over the disclosure of data.

4.1.2 Localization and Tracking

Localization and tracking are the threats of specifying and recording a person's location through time and space by different means such as cell phone location, Internet traffic or GPS data [40]. The availability of massive and complete spatial and spatiotemporal data has led to an increasing interest in using geographic data and incorporating spatial information analysis.

With the progress of the IoT system, several influences would apparently amplify the localization threats such as the expansion of location-aware applications and improvement of their accuracy, the ubiquity of data collection technology and interaction with IoT devices that record the identity, location and activity of the user.

4.1.3 Profiling

Profiling is the process of collecting and processing data about individuals' activities and actions over long periods to classify them according to some feature. The information is usually collected without permission from users and integrated with other personal data to create a more complete profile. Profiling is currently used in a large range of domains, for example, e-commerce, targeted advertising and credit scoring [41]. One of the risks associated with profiling is that personal information may be exposed to other users, as other users who share the same computer and browser may view one's targeted advertisement. Moreover, many users are disturbed by the mere awareness of being watched and tracked.

With the growth of the IoT, data collection incredibly increases quantitatively due to the explosion of data sources and connected devices. Furthermore, data will change also qualitatively as data is collected from previously inaccessible parts of people's private lives, for example, data collected by wearables and different devices at home [40].

4.1.4 Life-cycle Transitions

This kind of privacy threat refers to the disclosure of private information where the owner of a customer product is changed during its life cycle. Since consumer products that hold private information such as smartphones, cameras and laptops are mostly under the control of the same owner during their entire life cycle, this problem is not observed very often. However, as more and more everyday things will be connected

and will contain private data, the risk for privacy disclosure due to change of owner will increase [42].

4.1.5 Inventory Attack

Inventory attacks are related to the illegitimate gathering of information about the existence and characteristics of things in a specific place. Inventory attacks can usually be performed by using the fingerprint of IoT devices, for instance, their communication speed, reaction time and so on. If the promise of the IoT will be fulfilled, all smart things will be addressable over the Internet, opening the opportunity for unauthorized entities to exploit this and create an inventory list of things belonging to a target. An inventory attack could be used for profiling individuals, since owning special items disclose private information about the owner [40].

4.1.6 Linkage

Linkage threat refers to uncontrolled disclosure of information due to combining separated data sources and linking different systems. Integrating various types of information about the individual reveals new facts which are not expected by the owner. The revealed information is considered a privacy breach [41].

Within the IoT context, the linkage threat will be increased due to integrating different organizations that establish a more heterogeneous and distributed system which will increase the system complexity and makes data collection operation less transparent [40].

4.2 *Privacy-Preserving Solutions for IoT*

Preserving the privacy of IoT devices should be one of the main priorities for the successful adoption and development of the IoT system. There are several approaches which have been suggested to preserve privacy. This section provides a brief discussion of these approaches to address the privacy issue in the IoT system.

- **Privacy by Design:** One valuable key to preserving privacy in the IoT environment is the privacy by design. The IoT customers should have the required features to control their own information and define who can access it. Currently, some companies use a sort of agreement that allows certain services to access data as desired. Therefore, built-in tools to preserve user's privacy are required to be built as an essential part of any product.
- **Privacy Awareness:** One of the main problems of privacy violation is the lack of public awareness. IoT users have to be fully aware of how to keep themselves protected against any types of privacy threats [43].

- **Data Minimization:** IoT service providers should employ the concept of data minimization by reducing personal data collection to only what is related to the service they introduce. They also need to retain the data only if they need it for the service [44].
- **Cryptographic Techniques:** One of the main solutions to preserve the privacy in IoT devices is employing the appropriate cryptographic technique to encrypt data. However, with limited storage and computation resources in IoT devices, this solution may be difficult to achieve [45].
- **Data Anonymization:** It is necessary after data collection that all unique identifiers such as social security number and driving license numbers should be removed from data records to remove the identity of the individuals in databases.
- **Access Control:** Providing an efficient access control model for the IoT system to enable smart things to provide fine-grained decisions is one of the solutions for preserving the privacy of IoT users.

5 IoT Safety

The IoT safety is one of the highest priorities to prevent the IoT system and its elements from producing physical damage or undesirable threat and protect the surrounding environment from such damage. In addition, safety-critical operations should be protected to maintain reliability in the IoT system. Ensuring safety and reliability in the IoT system is not an easy task. It requires not only building a consistent application but also developing new design approaches. Safety and security affect each other. Safety is concerned with physical damage of IoT devices and its surroundings. It is obvious that the physical system attached to a computer system generates a larger surface attack than a pure computer system. It also provides side channels attacks that enable intruders to detect and manipulate the computer system. Moreover, safety issues amplify the magnitudes of traditional security attacks [46].

Safety and security are integrated together at the design phase of the product life cycle and at runtime check for either physical system or computer system. Since IoT devices are connected to the Internet and new threats are exploited every day, a runtime check is more important to identify new threats and looking for the best method to mitigate against. Hence, the system needs to be monitored during operation to detect various threats [46].

The safety in the IoT system should be considered since a device may work safely in normal use, but if the device is hacked, the attacker will try to manipulate the functionality of the device causing harm to objects controlled by the device or compromise people approaching into contact with it [47].

There are serious safety issues coming with open and unused ports of IoT devices as it allows attackers to inject malicious codes causing damages to devices especially safety-critical devices. Therefore, this issue should be addressed in future product design to maintain physical security and safety of IoT devices.

6 IoT Ethics

Ethics is a branch of philosophy that defines human conduct and behaviour in the society. Ethics considers what is morally right or wrong, just or unjust, while rationally justifying our moral judgments. Ethics in the IoT context deal with defining the correct regulation for human activities towards others and themselves; hence, ethics can be considered as a way to define what is good and bad, right and wrong. With the IoT growth, it will possibly give rise to other moral dilemmas, especially as the technology continues to outperform the development of regulations and policies. The IoT will change everything about how society works and plays. Therefore, there is a need to develop an ethical framework that helps ensure the IoT is used for the good of humanity and not the other way around.

Due to the complexity, heterogeneity and large scale of the IoT system, new ideas and thoughts should be presented to define the appropriate regulation and policies for this complex environment. Ethical issues in the IoT are mainly caused by the expansion of IoT technologies [49]. In addition, as the community continues to explore the risks and opportunities associated with IoT-driven systems, attention to transparency and the ethics of these systems' use and behaviour needs to be a core part of the discussion. In addition, building ethical frameworks are needed to help to understand what is appropriate and inappropriate and what is good and bad. The mechanisms that enforce ethical IoT frameworks need to be relevant to an ecosystem that includes humans, autonomous and self-determining systems, devices, and virtual and physical environments [50].

A strong ethical standard will motivate companies to design smarter and more inclusively to avoid algorithmic issues and ensure global connectivity. When it comes down to it, every company is responsible for maintaining an ethical IoT foundation or consumers will deny access to their information resulting in a data deficit for companies. To get this right, leaders must consider the capacity of their IoT technology and how they can expedite access worldwide [48].

6.1 *Ethical Design for IoT*

With billions of IoT devices, the amount of data generated by these devices will be unpredictable. Integrating this amount of data with innovations and developments of efficient and effective big data analytics tools will change the people thinking about IoT and the huge economic progress that can be achieved using this data. On the other hand, there is still a lack of the appropriate ethics that regulate how these data can be collected without violating people's privacy. Therefore, an ethical design for future IoT devices and services is required to open various ethical options for users within the digital platform and make it act as an added value where user pay for it if he/she is willing to apply [48].

The ethical design in the IoT products is used as a means to authorize IoT consumers to manage and protect their personal data and other related information. In other words, IoT users will have the complete freedom to define their own ethical choices while interacting with IoT devices. All various ethical options and choices will be embedded in the algorithms that are created by programmers and developers. These choices will include different degrees of privacy and data protection to allow users to choose what is best for their purposes [50]. Since providing these new features are not free, an ethical IoT device will include additional cost to involve the implementation and deployment of ethical framing and ensure a higher level of freedom to IoT users. It will be available for users to decide to pay for these new ethical features or not [51].

According to W. Pollard [52], IoT devices involving ethical design should have the following features:

- The ability to manage and control the collection and distribution of personal data or services.
- The ability to apply different rules and policies regardless of time and space.
- The ability to support dynamic contexts such as home and office.
- The ability to observe, recognize and support relationships that need ethical options.

6.2 *Ethics Challenges in IoT*

Although the IoT system has been widely accepted in our society and billions of devices are existing, there are several issues to apply ethics in the IoT context. These challenges include the following:

- **Owner Identification:** The accurate identification of the owner of the data collected in a typical IoT system is difficult to define. Collecting various types of data without the user's consent or permission is a critical issue that needs to be addressed in the IoT system.
- **Public and Private Border Line:** The IoT system involves multiple sensors that collect both public and private data. In the absence of well-defined boundaries for users' information, the line between private and public information must be cleared and defined in various IoT applications.
- **People's Life Attacks:** In a pure computer system, the security breach can lead to data loss or physical damage to the computer system. While in the IoT system, as all our environment including our home, car, smart meter, etc. are connected within the IoT network, the IoT breach can literally affect people lives directly. For instance, an attacker can control home energy and cause serious damage to people living in that home [53].

7 Case Study: Smart Cities

The concept of a smart city is used to describe the better use of public resources to improve people quality of life using the unlimited benefits provided by the IoT system and at the same time decreasing operational costs of public administrations. The IoT provides numerous advantages in controlling and optimizing public services, such as lighting, maintenance of public areas, transport and parking, preservation of cultural heritage, surveillance and garbage collection. Moreover, with multiple sensors existing everywhere and different types of data collected from these devices, people awareness can be improved regarding the status of their city and encourage the active participation of the citizens in the management of public administration [54].

In this section, we provide the smart city as a case study to discuss different security threats and suggest novel solutions to mitigate against.

7.1 *Security Threats in Smart Cities*

Like all other IoT applications, smart cities provide an extensive range of vulnerabilities that can be exploited by attackers and other malicious actors causing serious damage to either people or physical devices. The security threats in the context of a smart city should not be ignored as it can affect productivity and efficiency of services provided by the smart city. There are several security threats in smart cities, some of the most common threats involve the following:

- **Data and Identity Theft:** Data created by unprotected smart city infrastructures such as parking garages and surveillance can be used to provide attackers with a huge amount of data to steal personal information that can be exploited for fake transactions and identity theft.
- **MITM Attack:** It is one of the common threats in smart cities in which an attacker injects a malicious node between two communicating nodes to steal conversation information. In smart cities, MITM attack on a smart valve can be used to intentionally cause wastewater overflow.
- **Device Hijacking:** In this type of attack, the attacker captures and controls a certain device without changing its basic functionality which makes it very difficult to be detected. In a smart city context, an attacker can exploit hijacked smart meters to launch ransomware on energy management systems [53].
- **Insecure Hardware:** Sensors are the starting point of any attack. If they are not tested appropriately, they will create major threats to the entire IoT system. The lack of hardware standardization of IoT devices creates several weak points that can be exploited by attackers.
- **Larger Attack Surface:** The large scale of a smart city network creates a large attack surface. Since smart cities contain thousands of systems and devices to control various services, any device in the smart city network is vulnerable and

can be attacked at any time. In addition, attacking a single device can possibly compromise the entire network [55].

- **Software Bugs:** Since smart cities contain thousands of systems and devices, a simple software bug can have an enormous effect on the system devices and applications.

7.2 *Security Solutions for Smart City*

Providing various security mechanisms to secure a smart city is a mandatory operation to keep the innovation of new services and applications that improve people lives and the quality of their lives. There are a set of security solutions for building a secure smart city. These solutions involve: mutual authentication, security monitoring and analysis, and data integrity and confidentiality. This section provides an overview of these security solution. In addition, Table 1 provides a summary of various security threats in different sectors of smart cities and suggested solutions.

- **Mutual Authentication:** Various types of devices connected to a smart city network should be authenticated before any data transmission occurs. This will validate the identity of communicating devices and ensure only legal devices are permitted to send and receive data. So, mutual authentication, where two entities device and service validate their identity to each other, can help to protect against malicious attacks [56].
- **Security Monitoring and Analysis:** The system data should be captured and monitored to detect potential security violations or potential security threats. Once a security threat is detected, appropriate actions according to system security policy should be performed [53].
- **Data Integrity and Confidentiality:** Smart cities use data to improve services and quality of life for citizens. This data should be reliable and accurate. In other words, integrity measures should be employed to ensure data is accurate and no manipulation occurs through the transmission process. Moreover, security measures should be employed to protect against the unauthorized disclosure of sensitive information.

8 Conclusion

The IoT has the capability to connect and communicate with almost all real-world objects over the Internet to increase information sharing. With the help of sensors, the IoT has the ability to collect, analyse and deploy a huge amount of data which in turn will be converted into meaningful information and knowledge that can be used to create new application and services to improve our quality of life. Security and privacy are considered to be the major issues in the IoT system. Providing a secure and

Table 1 Security threats and suggested solutions in smart cities, structured from some data provided in [55]

Sector	Security threats	Solutions
Smart building	<ul style="list-style-type: none"> • Systems failure • Controlling the fire system • Altering smart meters • Opening parking gates • Infection by malware • Damaging or controlling the lifts • Disabling water and electricity supplies 	<ul style="list-style-type: none"> • Two-factor authentication • Threat and risk modelling • IoT forensics • Data backup and recovery solutions to guarantee reliability and continuity of services
Smart Transportation	<ul style="list-style-type: none"> • Sending wrong emergency messages • Stopping the vehicle's engine • Changing GPS signals • Disrupting the vehicle's emergency response system • Disrupting a vehicle's braking system 	<ul style="list-style-type: none"> • Misbehaviour detection solutions • Pseudorandom identities • Public key infrastructure (PKI), digital certificates (ECDSA) • Data encryption solutions (ECIES and AES)
Healthcare	<ul style="list-style-type: none"> • Sending wrong information • Sending an emergency alert • Jamming attacks • Eavesdropping sensitive information • Disrupting the monitoring system • Disrupting the emergency services 	<ul style="list-style-type: none"> • Secured Wi-Fi networks to guarantee safe handling of confidential information and personal data • Risk assessment
Energy	<ul style="list-style-type: none"> • Spoofing addresses and usernames • Unauthorized access and controls • Zero-day attacks • Denial of service and distributed denial of service (DDoS) 	<ul style="list-style-type: none"> • Intrusion detection and prevention techniques • Risk assessment • Insider threat analysis • Cybercrime intelligence

privacy-preserving IoT system should be a compulsory task to continue its successful developments in our environment. In addition, safety plays an important role in the IoT system to provide a safe and reliable system and protect the IoT system and its components from causing an unacceptable risk or physical damage. In the same way, ethics and regulations when dealing with IoT data are needed to be defined since the technology continues to outperform the development of current regulations and policies. This chapter provided an overview of IoT security, privacy, safety and ethics. It discussed the architecture and essential characteristics of the IoT system. It also presented IoT security by highlighting security requirements, security by design, security attacks and security challenges. IoT privacy by investigating privacy threats

and solutions to preserve privacy were also discussed. IoT safety and ethics were also discussed. In the end, a case study of the smart city was introduced to discuss security threats and suggested solutions to build a secure smart city.

References

1. Atlam, H.F., Walters, R.J., Wills, G.B.: Internet of things: state-of-the-art, challenges, applications, and open issues. *Int. J. Intell. Comput. Res.* **9**(3), 928–938 (2018)
2. Atlam, H.F., Walters, R.J., Wills, G.B.: Intelligence of Things: Opportunities & Challenges. 3rd Cloudification of the Internet of Things (CIoT), pp. 1–6 (2018)
3. Martin, P., Brohman, K.: CLOUDQUAL: a quality model for cloud services. *IEEE Trans. Ind. Inf.* **10**(2), 1527–1536 (2014)
4. Cerf, V., Ryan, P., Senegés, M., Whitt, R.: IoT safety and security as shared responsibility. *Bus. Inform.* **1**, 7–19 (2016)
5. Shanbhag, R., Shankarmani, R.: Architecture for internet of things to minimize human intervention. In: 2015 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2015, pp. 2348–2353 (2015)
6. Ashton, K.: That ‘Internet of Things’ Thing. *RFID J.*, 4986 (2009)
7. ITU: The Internet of Things. ITU Internet Rep., p. 212 (2005)
8. ITU: Overview of the Internet of things. Ser. Y Glob. Inf. infrastructure, internet Protoc. Asp. next-generation networks - Fram. Funct. Archit. Model., p. 22 (2012)
9. Guillemin, P., Friess, P.: Internet of things strategic research roadmap. *Eur. Comm. Inf. Soc. Media, Luxembourg* (2009)
10. Stallings, W.: The internet of things: network and security architecture. *Internet Protocol J.* **18**(4), 2–24 (2015)
11. Cisco: The Internet of Things Reference Model. White Paper, pp. 1–12 (2014)
12. Atlam, H.F., Alenezi, A., Walters, R.J., Wills, G.B., Daniel, J.: Developing an adaptive Risk-based access control model for the Internet of Things. In: 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), no. June, pp. 655–661 (2017)
13. Iqbal, M.A., Olaleye, O.G., Bayoumi, M.A.: A review on internet of things (IoT): security and privacy requirements and the solution approaches. *Global J. Comput. Sci. Technol.: E Network, Web & Secur.* **16**(7) (2016)
14. Atlam, H.F., Alenezi, A., Hussein, R.K., Wills, G.B.: Validation of an adaptive risk-based access control model for the internet of things. *Int. J. Comput. Network Inf. Secur.*, 26–35 (2018)
15. Maple, C.: Security and privacy in the internet of things. *J. Cyber Policy* **2**(2), 155–184 (2017)
16. Yu, Y., Kaiya, H., Yoshioka, N., Hu, Z., Washizaki, H., Xiong, Y., Hosseinian-Far, A.: Goal modelling for security problem matching and pattern enforcement. *Int. J. Secure Softw. Eng. (IJSSE)* **8**(3), 42–57 (2016)
17. Suo, H., Wan, J., Zou, C., Liu, J.: Security in the internet of things: a review. In: International Conference on Computer Science and Electronics Engineering (CCSEE 2012) vol. 3, pp. 648–651 (2012)
18. Abdur, M., Habib, S., Ali, M., Ullah, S.: Security issues in the internet of things (IoT): a comprehensive study. *Int. J. Adv. Comput. Sci. Appl.* **8**(6) (2017)
19. Theobald, M.: The Importance of Security by Design for IoT Devices (2018). <https://www.redalertlabs.com/blog/the-importance-of-security-by-design-for-iot-devices>. Accessed 20 Aug 2018
20. James, M.: Secure by Design: Improving the cybersecurity of consumer Internet of Things Report (2017)

21. George, C., Fink, G.A., Mandal, S., Hrivnak, C.: Internet of things (IoT) security best practices. IEEE Internet Technol. Policy Community White Paper, no. February (2017)
22. Atlam, H.F., Alenezi, A., Alharthi, A., Walters, R., Wills, G.B.: Integration of cloud computing with internet of things: challenges and open issues. In: 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), no. June, pp. 670–675 (2017)
23. Kvarda, L., Hnyk, P., Vojtech, L., Neruda, M.: Software implementation of secure firmware update in IoT concept. Adv. Electrical Electron. Eng. **15**(4), 626–632 (2017)
24. Venkatesh, J., Diego, S.: Scalable- application design for the IoT. IEEE Comput. Soc., 62–70 (2017)
25. Babar, S., Stango, A., Prasad, N., Sen, J., Prasad, R.: Proposed embedded security framework for Internet of Things (IoT). In: 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), no. May 2014 (2011)
26. Sopori, D., Pawar, T., Patil, M., Ravindran, R.: Internet of things: security threats. Int. J. Adv. Res. Comput. Eng. Technol. (IJARCET) **6**(3), 263–267 (2017)
27. Deogirikar, J.: Security attacks in IoT : a Survey. In: International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), pp. 32–37 (2017)
28. Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S.L., Kumar, S.S., Wehrle, K.: Security challenges in the IP-based Internet of Things. Wireless Personal Commun. **61**(3), 527–542 (2011)
29. Khoo, B.: RFID As an enabler of the internet of things: issues of security and privacy. In: IEEE International Conferences on Internet of Things and Cyber, Physical and Social Computing (iThings/CPSCom 2011), pp. 709–712 (2011)
30. Mitrokotsa, A., Rieback, M.R., Tanenbaum, A.S.: Classifying RFID attacks and defenses. Inf. Syst. Front. **12**(5), 491–505 (2010)
31. Raju, I., Parwekar, P.: Detection of sinkhole attack in wireless sensor network. Adv. Intell. Syst. Comput. **381**(July), 629–636 (2016)
32. Padhy, R., Patra, M., Satapathy, S.: Cloud computing: security issues and research challenges. Int. J. Comput. Sci. Inf. Technol. Secur. (IJCSITS) **1**(2), 136–146 (2011)
33. Atlam, H.F., Attiya, G., El-Fishawy, N.: Integration of color and texture features in CBIR system. Int. J. Comput. Appl. **164**(3), 23–29 (2017)
34. Aman, W.: Modeling adaptive security in IoT Driven eHealth. In: Norwegian Information Security Conference (NISK 2013), pp. 61–69 (2013)
35. Atlam, H.F., Walters, R.J., Wills, G.B.: Fog computing and the internet of things: a review. Big Data Cognitive Comput. **2**(2), 1–18 (2018)
36. Atlam, H.F., Walters, R.J., Wills, G.B.: Internet of nano things : security issues and applications. In: 2018 2nd International Conference on Cloud and Big Data Computing, no. October, pp. 71–77 (2018)
37. Westin, A.F.: Privacy and Freedom. Atheneum, New York (1967)
38. Padilla-López, J.R., Chaaroui, A.A., Flórez-Revuelta, F.: Visual privacy protection methods: A survey. Expert Syst. Appl. **42**(9), 4177–4195 (2015)
39. Atlam, H.F., Alenezi, A., Alassafi, M.O., Walters, R.J., Wills, G.B.: XACML for building access control policies in internet of things. In: Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security (IoTBDs 2018), pp. 253–260. (2018)
40. Ziegeldorf, J.H., Morchon, O.G., Wehrle, K.: Privacy in the internet of things: Threats and challenges. Secur. Commun. Netwo. **7**(12), 2728–2742 (2014)
41. Toch, E., Wang, Y., Cranor, L.F.: Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems. User Model. User-Adapted Interact. **22**(1–2), 203–220 (2012)
42. Aleisa, N., Renaud, K.: Privacy of the internet of things: a systematic literature review (Extended Discussion). ArXiv e-prints, pp. 1–10 (2016)

43. Atlam, H.F., Attiya, G., El-Fishawy, N.: Comparative study on CBIR based on color feature. *Int. J. Comput. Appl.* **78**(16), 975–8887 (2013)
44. Singh, J., Pasquier, T., Bacon, J., Ko, H., Eysers, D.: Twenty security considerations for cloud-supported internet of things. *IEEE Internet Things J.* **3**(3), 269–284 (2016)
45. Atlam, H.F., Alenezi, A., Walters, R., Wills, G.B.: An overview of risk estimation techniques in risk-based access control for the internet of things. In: *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDs 2017)*, pp. 254–260 (2017)
46. Wolf, M., Serpanos, D.: Safety and security of cyber-physical and internet-of-things systems. *Proc. IEEE* **105**(6), 983–984 (2017)
47. Hussein, R.K., Alenezi, A., Atlam, H.F., Mohammed, M.Q., Walters, R.J., Wills, G.B.: Toward confirming a framework for securing the virtual machine image in cloud computing. *Adv. Sci. Technol. Eng. Syst.* **2**(4), 44–50 (2017)
48. Popescu, D., Georgescu, M.: Internet of things—some ethical issues. *USV Ann. Econ. Public Adm.* **13**(2), 208–214 (2013)
49. Alenezi, A., Zulkpli, N. H.N., Atlam, H.F., Walters, R.J., Wills, G.B.: The impact of cloud forensic readiness on security. In: *7th International Conference on Cloud Computing and Services Science*, pp. 511–517 (2017)
50. Baldini, G., Botterman, M., Neisse, R., Tallacchini, M.: Ethical design in the internet of things. *Sci. Eng. Ethics* **24**(3), 905–925 (2018)
51. Atlam, H.F., Alenezi, A., Alassafi, M.O., Wills, G.B.: Blockchain with internet of things: benefits, challenges, and future directions. *Int. J. Intell. Syst. Appl.* June, pp. 40–48 (2018)
52. Pollard, W.: IoT governance, privacy and security issues. *Eur. Res. Clust. Internet Things*, 23–31 (2015)
53. Zanella, A., Bui, N., Castellani, A., Vangelista, L., Zorzi, M.: Internet of things for smart cities. *IEEE Internet Things J.* **1**(1), 22–32 (2014)
54. Ijaz, S., Ali, M., Khan, A., Ahmed, M.: Smart cities: a survey on security concerns. *Int. J. Adv. Comput. Sci. Appl.* **7**(2) (2016)
55. Kitchin, R., Dodge, M.: The (In)Security of smart cities: vulnerabilities, risks, mitigation, and prevention. *J. Urban Technol.*, 1–19 (2017)
56. Khatoun, R., Zeadally, S.: Cybersecurity and privacy solutions in smart cities. *IEEE Commun. Mag.* **55**(3), 51–59 (2017)