Wireless Personal Communications (2019) 108:325–344
https://doi.org/10.1007/s11277-019-06405-y

A Review of Security in Internet of Things

Yasmine Harbi[1] · Zibouda Aliouat[1] · Saad Harous[2] · Abdelhak Bentaleb[3] · Allaoua Refoufi[1]

Published online: 24 April 2019

Abstract

Internet of Things (IoT) has drawn significant attention in recent years since it has made revolutionary changes in human life. The IoT enables the exchange of information in a wide variety of applications such as smart buildings, smart health, smart transport, and so on. These diverse application domains can be unified into a single entity referred as smart life. The rapid evolution of the IoT has pushed a race between cyber-criminals and security experts. As billions of connected things communicate with each other and can exchange sensitive information that may be leaked. Hence, strengthening IoT's security and preserving users' privacy is a major challenge. This paper aims to provide a comprehensive study of the IoT security. Several IoT security attacks are analyzed, and a taxonomy of the security requirements based on the attacks' purposes is proposed. Moreover, recent security solutions are described and classified based on their application domains. Finally, open research directions and security challenges are discussed.

Keywords IoT · Smart life · Cyber-attacks · Security · Privacy

✉ Saad Harous
harous@uaeu.ac.ae

Yasmine Harbi
yasmine.harbi@univ-setif.dz

Zibouda Aliouat
zaliouat@univ-setif.dz

Abdelhak Bentaleb
bentaleb@comp.nus.edu.sg

Allaoua Refoufi
allaoua.refoufi@univ-setif.dz

[1] LRSD Laboratory, Ferhat Abbas University of Setif1, Sétif, Algeria

[2] College of Information Technology, United Arab Emirates University, Al Ain, UAE

[3] National University of Singapore, Singapore, Singapore

1 Introduction

The concept of the Internet of Things has been introduced by Kevin Ashton in 1999. IoT aims to connect anything at anytime in anyplace [1]. Things in the IoT include physical objects from tiny to very large machines that seamlessly communicate with each other via the Internet without human intervention [2]. The IoT devices are equipped with sensors to capture data and actuators to autonomously and intelligently perform actions [3]. Figure 1 highlights various examples of the IoT devices.

Over the past few years, the IoT has gained significant attention since it brings potentially tremendous benefits to the human. The IoT spans many diverse application domains such as home automation, environmental monitoring, healthcare, and so on [4]. The primary objective of the IoT is unification of these numerous diverse application domains under the same umbrella referred as smart life [4].

Shortly, billions of devices expected to be connected to the Internet [5]. Hence, an increasingly massive amount of data will flow within the Internet [6]. This data can face various security attacks such as eavesdropping and altering. Consequently, the user's privacy will be threatened [7]. For example, an adversary can intercept a baby monitor system using a Software Defined Radio (SDR) in order to compromise the user's privacy [8].

The IoT combines different existing technologies like Wireless Sensor Network, Radio Frequency IDentification, cloud computing, Constrained Application Protocol, etc. Therefore, it inherits the security flaws of each technology [9]. Some available technologies are illustrated in Fig. 2.

- Wireless Sensor Network (WSN) consists of a large number of physical autonomous sensors deployed in the environment in order to control the environmental conditions [1]. The WSNs are prone to various type of attacks such as sinkhole and wormhole attack, node tampering and jamming, etc [6].
- Radio Frequency IDentifiaction (RFID) is used to identify and track IoT objects. It allows data exchange via radio signals over a short distance [1]. Similar to the WSN, the RFID technology has many vulnerabilities including spoofing, cloning, and sniffing [6].

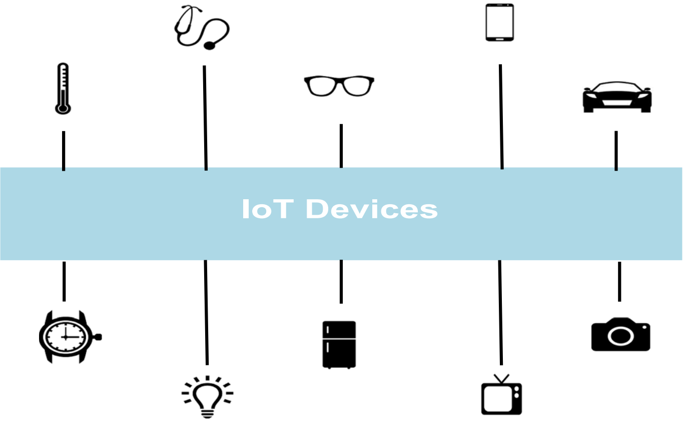


Fig. 1 Examples of IoT devices

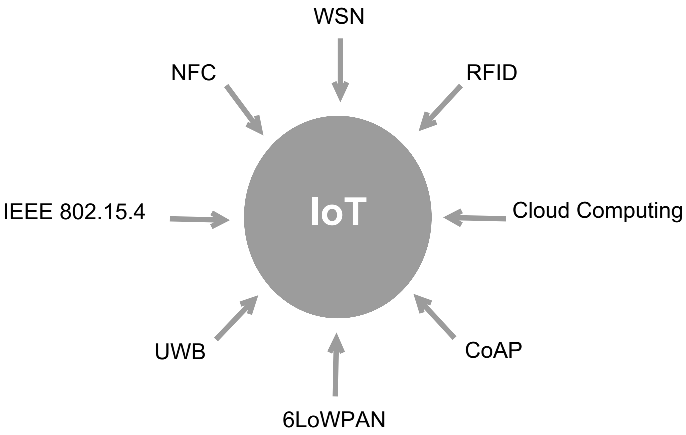


Fig. 2 IoT enabling technologies

- Cloud computing plays an important role in the IoT by offering an unlimited storage ressources and processing power [10].
- Constrained Application Protocol (CoAP) is an application layer protocol proposed for ressource-constrained devices [11, 12].
- IPv6 Low power Wireless Personal Area Network (6LoWPAN) combines IPv6 and LoWPAN and allows transmission of IPv6 packets over IEEE 802.15.4 networks [11]. The 6LoWPAN is suitable for the IoT and has several advantages. However, it is susceptible to various attacks like DoS (Denial of Service) and eavesdroping attacks [13].
- Ultra WideBand (UWB) is a viable technology for a wide variety of IoT applications due to its low power consumption, higher precision, and security [14].
- IEEE 802.15.4 is a protocol for the physical layer and the MAC (Medium Access Control) layer in Wireless Personnal Area Networks (WPANs). It provides the connection of things in personal area with low energy consumption [11].
- Near Field Communication (NFC) is a short range technology that can be used in various IoT systems such as payments and authentication. The NFC provides easy network access and data exchange. However, it is prone to information leakage since the wireless signal generated by device can be picked up by an attacker [15, 16].

Securing the IoT is a challenging task. Nevertheless, most of IoT devices are designed in small size and inherently have limited resources (i.e. battery, processing, and storage). The implementation of conventional security mechanisms is infeasible since it requires a very complex and hard process [17, 18]. The major challenge is to develop a lightweight security mechanism for highly constrained devices.

This paper presents an analysis of the IoT security vulnerabilities and threats. Then, we provide a taxonomy of the IoT security requirements based on the attacks' purposes. In addition, we describe various recent security solutions and classify them based on their application domains. Finally, we discuss open research issues and challenges of the IoT security.

The rest of this paper is organized as follows. Section 2 presents the related work and highlights our work with respect to the cited surveys. Section 3 analyses different types of attacks in the context of IoT. The taxonomy of the IoT security requirements is provided in

Sect. 4. Various recent IoT security solutions are described in Sect. 5. Section 6 discusses future directions and challenges of the IoT security and concludes our study.

2 Related Work

Several surveys were published recently to discuss the IoT security. Even though a number of issues were addressed but not all of them. None of these surveys has detailed all the security concerns of IoT. In our work, we analyse different security threats and offer a taxonomy of the security requirements according to the IoT attacks' purposes. This taxonomy aims to achieve a secure IoT environment. Table 1 illustrates a comparative analysis of the cited surveys.

In [19], the authors presented an IoT security roadmap including privacy, trust, identification, and access control. First, they detailed a systemic and cognitive approach of IoT proposed in [26]. The authors considered their vision more convenient and flexible compared to the layered approach. They explained the components and interactions of the approach and highlighted its efficiency by using it in smart manufacturing. Then, they discussed a state-of-the-art and taxonomy of the security concerns, exposed meaningful solutions, and suggested different research directions. Finally, they illustrated relevant standardization activities for the IoT security. Although the survey was interesting, it analyzed only the security issues that may occur on the interactions of their approach and did not consider the other IoT security concerns such as integrity, confidentiality, and availability.

Authors in [20] presented current IoT standards and their security objectives. They provided some security requirements to secure IoT devices and data. Then, they reported different IoT-enabled technologies and protocols for each IoT layer: the perception, the network, and the application layer. The technologies vulnerabilities including WSN and RFID weaknesses were identified, and some solutions were presented. Concerning the security issues, they focused on data confidentiality, integrity, availability, and privacy. They also discussed the security challenges and some solutions. However, they did not detail in depth the enabling technologies vulnerabilities. Also, they did not grant attention to authentication, access control and trust which are important key issues in the context of IoT security.

Yang et al. [21] presented a survey on security and privacy issues for IoT systems and applications. Their work is composed of four parts. Firstly, they explored the two main IoT devices limitations: battery power and computing power. Then, they discussed possible solutions for battery life extension and lightweight computing, and exposed some existing security mechanisms for constrained devices. Secondly, they presented a classification on IoT attacks according to [9, 27]. Thirdly, the authors focused on authentication and access control schemes and architectures for IoT systems. Finally, they discussed the security problems and solutions in the perception layer, network layer, transport layer, and application layer. In this work, the authors discussed the security and privacy issues in IoT. Nevertheless, they were limited to authentication and access control. Therefore, many relevant security issues were neglected such as confidentiality, privacy, and integrity. Also, they did not provide enough details about the IoT attacks.

In [22], the authors cited some IoT security attacks and detailed the perception, the network, and the application layers. Then, they treated the security issues and attacks of different layers and provided possible countermeasures. Subsequently, the authors presented some solutions proposed by different companies and organizations. Finally, they concluded their work by discussing future directions. The authors studied the state-of-the-art of

Table 1 Comparative analysis of the cited surveys

Survey	References	IoT vision	Security concerns
The roadmap for security challenges in Internet of Things	[19]	Person, process, intelligent object, and technological ecosystem	Privacy, trust, access control, authentication
Internet of Things: survey on security and privacy	[20]	3 layers: perception, network, and application	Confidentiality, integrity, availability, privacy
A survey on security and privacy issues in Internet of Things	[21]	4 layers: perception, network, transport, and application	Authentication, access control
Internet of Things security	[22]	5 layers: perception, network, middleware, application, and business	Authentication, confidentiality
Security in Internet of Things: a survey	[23]	Physical things and virtual things	Confidentiality, integrity, authentication
Internet of Things security: a survey	[24]	3 layers: perception, network, and application	Authentication, authorization, privacy, trust
Security issues in the Internet of Things (IoT): a comprehensive study	[25]	Not mentioned	Authentication, access control, privacy, and confidentiality
Our survey	–	3 layers: physical, network, and application	Data security (i.e. confidentiality, privacy, integrity), communication security (i.e. authentication, access control, non-repudiation), device security (i.e. trust, availability)

security in the context of IoT. However, they defined the security problems superficially without presenting existing solutions in the literature. Furthermore, the security measures were not discussed in detail. The main limitation of this survey is that the authors did not cover many important security issues such as data privacy, integrity and access control.

Oracevic et al. [23] defined the security issues in IoT. They considered three main security requirements: confidentiality, integrity, and authentication. Then, they presented some recent IoT security solutions, and discussed possible directions for future research in the field of IoT security. The advantage of this work is the classification of the IoT security solutions. The main limitation of this survey is that the authors were limited to basic security requirements, and neglected other important security problems such as privacy, trust, access control, and availability. Moreover, they did not detail in depth the considered security issues.

In [24], authors presented security threats and vulnerabilities in IoT, and discussed existing solutions to mitigate these security flaws. First, they presented an overview of the IoT and the differences between the IoT security issues and the traditional network ones. They detailed the three layers of IoT (application, network, and perception) and highlighted the security threats that may face the components of each layer. Then, the authors discussed several solutions for the IoT threats and vulnerabilities. Next, they described a new taxonomy of the IoT security based on current security threats in the IoT applications, architecture, communication, and data. They also suggested an IoT architecture that enhances the network security. Finally, they discussed possible attacks caused by the security flaws, future directions, and security challenges. This survey provides a comprehensive analysis of the IoT security threats. One limitation of this work is the IoT security taxonomy remains unclear.

Authors in [25] discussed the IoT applications including industry, healthcare, and smart home. Then, they highlighted the major security requirements in IoT: authentication, access control, privacy, and confidentiality. Next, they focused on security threats, particularly in a smart home, classified these attacks into four levels according to their consequences, and suggested some possible countermeasures. The authors highlighted the major security issues in the IoT. The drawback of this survey is that the authors treated the security requirements superficially without presenting any existing solutions. Also, they did not describe most of the mentioned attacks.

3 IoT Security Threats

The IoT is evolving very fast, and the security attacks are advancing as well. To include the security requirements carefully into the IoT systems, it is firstly necessary to analyze the IoT vulnerabilities and attacks. The IoT devices are prone to various types of attacks since the IoT combines different existing technologies like WSN, RFID, cloud computing, etc. Therefore, it inherits the security flaws of each technology. In this section, we analyze different IoT security attacks and their purposes. This analysis is summarized in Table 2.

From Table 2, it is clear that the IoT devices are prone to various types of attacks. Also, we remark that different attacks have mainly the following purposes:

- Access to sensitive or private information.
- Control the communication.
- Damage the connected IoT devices and affect the services' availability.

Table 2 IoT security attacks

Attack	Technique/method	Purposes
Node tampering [28, 29]	Replace physically the sensor node or part of its hardware	Access to sensitive information Affect the services' availability
Node injection [9, 22]	Deploy physically malicious nodes in the IoT network	Control data flow Access to private information Launch additionnal attacks
Replay attack [28, 30]	A malicious node eavesdrops the communication and retransmits the packets received by a legitimate source host to the destination host	Obtain the confidence and trust of the IoT system
Sinkhole attack [31]	A compromised node claims unconstrained capabilities (i.e. power, processing, and communication) so that it is selected for forwarding all traffic from WSN nodes	Breach the data confidentiality Can launch additional attacks
Wormhole attack [32]	Two malicious nodes in different locations create a false one-hop transmission (tunnel) between them, even if they are located far away from each other. Hence, more data will be delivered through this tunnel	Breach the data confidentiality Can launch additional attacks
Code injection [9, 22, 33]	Inject malicious code that will be executed by the IoT system	Control the whole system Compromise data integrity, privacy and correctness
Node jamming [34]	It is a subset of Denial of Service attacks. It can be implemented on WSNs, where the attacker can jam the signals by sending noise	Make intentional interferences in the network Disable the network
Social engineering [9, 35]	Based on human interaction. The attacker manipulates or influences the users of the IoT system	Access to confidential information
Sleep deprivation [9, 36]	Break the programmed sleep routines of IoT devices and keep the sensor nodes awake all times	Drain the devices' resources Make the IoT system dysfunctional
Man in the middle [37, 38]	Intercept secretly the communication between two nodes	Eavesdrop, alter or control the communication Take down the system
Denial of Service [39–41]	Send packets to the IoT system	Exhaust the service provider resources Disable the network Compromise data acquisition
RFID Sniffing [42, 43]	Sniff out or eavesdrop the data flow in the RFID technologies using various sniffing applications	Disclosure the data flow
RFID Spoofing [9, 44]	Spoof or imitate valid RFID information and send data with the valid tag ID in order to mask the attacker identity	Elicit sensitive data Gain access to the system by pretending the original source

Table 2 (continued)

Attack	Technique/method	Purposes
RFID Cloning [9, 45]	Clone an RFID tag by duplicating data from a pre-existing RFID tag	Gain access to the system by cloning an existing node
Sybil attack [46, 47]	Pretend the identities of many other nodes. So, the attacker can be in more than one location	Degrade the data security and resource utilization
Phishing attack [48]	Trick IoT devices or users usually by disguising as trustworthy entity	Gain access to sensitive information by tricking IoT devices or users
Encryption attack [9, 36, 49]	Use particular techniques like timing, power, fault and electromagnetic analysis on the IoT devices to find the encryption key	Find the encryption key and break the encrypted system
Malicious software [9, 50]	Infect or cripple an RFID system with malicious software like virus, worms, trojan horse, etc.	Damage connected IoT devices and components Tamper and steal information

4 IoT Security Requirements

According to the three essential attacks' purposes listed in the previous section, we classify the IoT security into three categories: data security, communication security, and device security (see Fig. 3).

To preserve sensitive information, we have to secure the data collected by the IoT devices. Also, we must secure the communication between these devices to avoid controlling the data flow by an adversary. In some IoT environments, the physical objects communicate with each other to provide intelligent services for human. Therefore, it is highly important to secure these devices.

4.1 Data Security

The IoT devices monitor the physical environments and transmit the collected data through wireless channels. However, this transmitted data is exposed to different security threats like eavesdropping and altering. To secure data in the context of IoT, we must preserve its confidentiality, privacy, and integrity.

Data confidentiality is the process of hiding private information from the unauthorized IoT objects [20, 51]. According to [52], data confidentiality is a fundamental issue that needs a lot of attention. Standard encryption mechanisms cannot be implemented directly for the IoT system since IoT devices have limited resources [53]. In order to provide data protection and confidentiality, the authors in [54] proposed the use of lightweight cryptographic algorithms. The work in [55] described some cloud-based solutions that secure channels and protect critical information. The authors in [56] indicated that applying privacy-based designs can increase the confidentiality levels.

Privacy includes the concealment of personal information and the ability to control what happens with such information [57]. Data privacy must be analyzed during data collection,

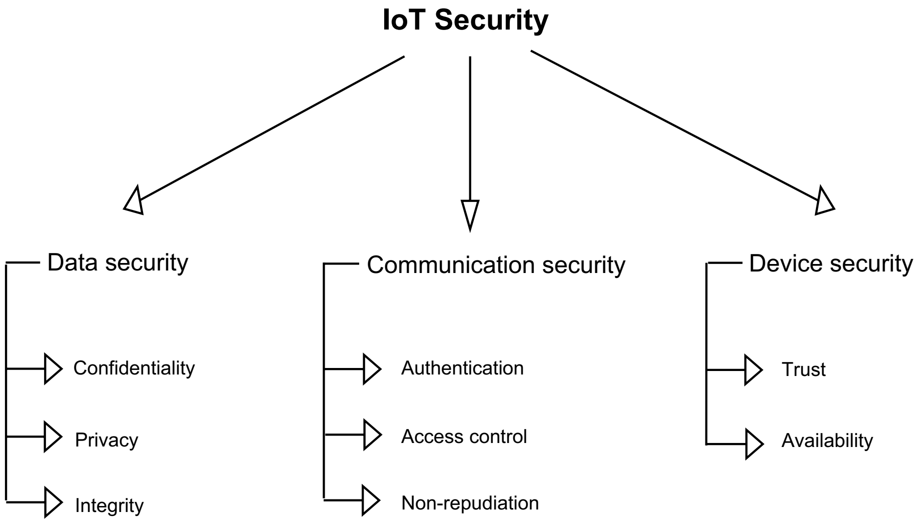


Fig. 3 IoT security taxonomy

transmission, and storage. Many practical solutions have been proposed to deal with data privacy. These techniques include anonymization, pseudo-random number generators, block ciphers, and stream ciphers [19].

- Anonymization-based solutions like K-anonymity [58], L-diversity [59], and T-closeness [60].
- Pseudo-random number generators were used to secure IoT devices by producing a random output sequence. Numerous lightweight pseudo-number generators are proposed for RFID tags such as works [61–63].
- Blocks ciphers transform a plain binary text of a fixed length (block) into a ciphertext with the same length using a symmetric key. Several lightweight blocks ciphers mechanisms are proposed for IoT such as [64–66].
- Contrary to blocks ciphers, stream ciphers transform the entire plain text into cipher one using a pseudo-random key stream (i.e. XORing plain text and key stream). The techniques presented in [67–69] are lightweight stream ciphers for constrained devices.

Data integrity ensures that the data to be received has not been altered or modified during transmission [51]. Integrity involves maintaining the consistency, accuracy, and trustworthiness of the data. Several cryptographic hash algorithms (e.g. MD5 and SH1) are used to ensure data integrity. However, most of these mechanisms cannot be implemented because the IoT devices are inherently resource constrained [70]. To address this concern, various lightweight hash functions were proposed like [71–73]. In case of detection of tampering data, error correction mechanisms such as Cyclic Redundancy Checks (CRC) and checksum functions can be used to solve the problem [9].

4.2 Communication Security

Before any communication between IoT devices, an authentication process is required. Thus, only authorized devices can access to systems or information. Moreover, non-repudiation in the communication is achieved.

Authentication is the process of validating an identity using login and other information like password, PIN and digital certificates [19]. It is required between two or group of parties in order to secure communication in IoT system. The authentication ensures that only authorized users can access the IoT devices and achieves non-repudiation in communications. When a new device is connected to the network, it should authenticate itself before exchanging data. The authentication can be verified using lightweight cryptographic algorithms, physical primitives, or biometric identification [74, 75].

Access control is a security feature that verifies the permission granted to users and systems to perform operations on other systems and resources [76]. The authors in [19] divided access control algorithms in five distinct types: role-based, organization-based, capability-based, attribute-based, and trust-based algorithms.

- The Role-Based Access Control (RBAC) [77] ensures authentication and access control using Elliptic Curve Cryptography (ECC) with an ephemeral private key to establish a session between a user and an object.
- The Organization-Based Access Control (OrBAC) model is an extension of RBAC. The authors in [78] proposed an authorization access model called SmartOrBAC that

enhances the OrBAC model by distributing authorization decisions among the constrained devices.

- In the Capability-Based Access Control (CapBAC) schemes, a capability is defined as a key that gives permission to access an object [79]. Several CapBAC solutions are proposed for IoT system such as [76, 80, 81].
- In Attribute-Based Access Control (ABAC), the user must present correct attributes to access a resource or some data [19].
- Trust-Based Access Control (TBAC) is an approach that considers a trust value to decide whether an entity can be accessed or not [19]. The authors in [82] proposed a Fuzzy Trust Based Access Control approach for the IoT devices where the trust value is based on experience, knowledge, and recommendation.

In the context of the IoT, non-repudiation is an essential element of network security [83]. It is the ability to ensure that an IoT node cannot repudiate having sent a message and that the receiver cannot deny having received the message [51]. The non-repudiation is particularly important in the business field (e.g. for digital contracts). It ensures that communications between two parties are valid and authentic. It can be achieved using Public Key Cryptography (PKC) [84].

Since small computing devices are not able to deal with large key size, alternative public-key cryptographic schemes may be used like Elliptic Curve Cryptography (ECC) [85] and Hyper-Elliptic Curve Cryptography (HECC) [86].

4.3 Device Security

To provide security in a critical environment, ensuring trust and confidence between interacting nodes is a primordial task. Furthermore, the availability of the IoT devices is highly required.

Trust is crucial for IoT users as stated in [87]. Trust management is the process of making decisions about communication with unknown entities [88]. In order to secure IoT system, it is necessary to interact with trusted IoT devices in order to prevent unwanted actions conducted by malicious nodes. According to [19], the trust management techniques are divided into two main categories: deterministic and non-deterministic trust. The deterministic trust encompasses policy-based and certificate-based mechanisms, while the non-deterministic trust includes recommendation-based, reputation-based, prediction-based, and social network-based systems.

The policy-based mechanisms use a set of policies to identify trust. In certificate-based approachs, trust is determined using public or private keys and digital signatures.

The recommendation-based systems utilize prior information to define trust. If there is no prior information, the prediction-based methods can be used.

To determine trust, the reputation-based systems employs global reputation of entities, while the social network-based ones consider the entities' social reputation.

Device availability is an important factor in IoT systems since they can be utilized in crucial areas including economy, industry, healthcare, etc [89]. According to [11], the availability of IoT networks should be performed in hardware and software. Hardware availability of the IoT application means the existence of all devices all the time, while software availability is the ability of providing services anywhere and anytime.

The IoT devices may face several attacks as DoS and DDoS that can hinder the services provided or affect the network availability [90]. The authors in [40] suggested a Service

Oriented Architecture (SOA) in order to prevent DDoS attacks in IoT systems. The work in [89] describes an Intrusion Detection System (IDS) that efficiently detects DoS attacks in IoT. Suo et al. [91] emphasize the importance of recovery after DDoS attacks.

5 IoT Security Solutions

In this section, we describe some recent solutions that have been proposed for securing the IoT in different application domains. The summary of these solutions is provided in Table 3.

In [92], the authors proposed an Intelligent Security Framework for IoT Devices that ensures authentication and data confidentiality. It is based on symmetric and asymmetric key encryption where the key pair is generated using Learning With Errors (LWE) mechanism introduced by Regev [93]. The proposed IoT architecture is composed of IoT nodes, device Gateway, service Gateway, master key repository, and the Cloud. The IoT nodes, the device gateway, and the service gateway have a unique ID. They exchange data using symmetric key encryption. The asymmetric key encryption is used to interact with the master key repository. This latter is the main entity of the framework since it generates the key pair of the IoT nodes, device gateway, and service gateway based on their unique ID. The proposed scheme is able to withstand DoS attacks, eavesdropping or man in the middle attack, and Quantum attacks.

Authors in [94] presented a lightweight communication protocol called Chaos-based Privacy Preservation (CPP) for securing smart home system. The proposed smart home design consists of agents (sensors, actuators, and monitors) and server (the central controller). The agents send data periodically to the central controller that returns responses and commands. The data is ciphered by a symmetric key which is generated using chaos-based system. This symetric key is updated on each data transmission phase. In addition, the authors employed Message Authentication Code (MAC) to verify the data integrity and authenticity. Security analysis shows that the proposed protocol ensures data confidentiality, privacy, integrity, and authenticity with reduced computational complexity, memory cost, and communication overhead.

Fragen et al. [95] have designed an access control scheme for Industrial Wireless Sensor Networks (IWSN) using certificateless signcryption. Their network architecture includes sensor nodes, users, gateway, and service provider. After deployment of the IWSN, the service provider gives a key pair (secret and public) to the sensor nodes. When the user wants to access to the IWSN, it should register with the service provider that sends back a partial private key. After receiving this key, the user computes the full private key which is used to encrypt the communication with the gateway. To access a sensor node's data, the user sends an encrypted query message and its public key to the gateway. This latter checks the user's public key and forwards the message to the sensor node. The transmitted data is encrypted using a symmetric key known to the sensor node and the user. The proposed scheme achieves a secure communication between the users and sensor nodes with enhancements in computational cost and energy consumption.

In [96], the authors proposed a secure smart shopping system using Ultra High Frequency (UHF) RFID. In this system, all items are equipped with RFID tags, while smart shelves and smart carts are equipped with RFID readers. In addition to the UHF RFID reader, the smart cart contains an LCD touch-screen as user interface, a Zig-Bee adapter to communicate with the server, a microcontroller for data processing, and a weight sensor

Table 3 Classification of the IoT security solutions

System	Technologies	Objectives	Domain
Intelligent security framework [92]	Symmetric and asymmetric encryption using lattice-based cryptography	To address privacy and confidentiality in the IoT	Smart environment
CPP [94]	Symmetric encryption using chaos-based cryptography, Message Authentication Code	To achieve privacy preserving in communication protocol	Smart home
Certificateless access control scheme [95]	Certificateless signcryption	To design a secure access control for IWSNs	Industrial IoT
Secure smart shopping system [96]	Symmetric and asymmetric encryption based on ECC, Message Authentication Code	To propose a secure smart shopping system	Smart environment
LDAC-KS [97]	Lightweight encryption/decryption using pairing-based cryptography	To preserve medical data privacy and facilitate secured data retrieval	Healthcare
Lightweight mutual authentication protocol [98]	Lightweight public key encryption	To design a secure mutual authentication protocol for resource constrained devices	Smart city

for weighting items. To secure communication with the server, the authors combined symmetric and asymmetric encryption/decryption based on ECC. Firstly, the smart cart signs or encrypts the message request with its private key, then with the server public key, and sends it to the server. This message request contains the smart cart ID, product tag information, time stamp, and two symmetric session keys. Secondly, the server decrypts the message request and verifies the signature and the time stamp. Then, it encrypts the message response and creates a Message Authentication Code (MAC) using the two shared symmetric keys. The encrypted message response and the MAC are sent to the smart cart. Finally, billing information generated by the smart cart is paid by costumer at checkout, and items' stock is updated by the smart shelves. The proposed system ensures data confidentiality and integrity and resists replay attacks.

Yang et al. [97] focused on distributed access control for health IoT system with preserving patient's information privacy. The proposed architecture contains a Body Sensor Network (BSN), home rehabilitation system, hospitals, attribute authorities, Auxiliary Computation Center (AAC), cloud server, and users. The presented scheme Lightweight Distributed Access Control system with Keyword Search (LDAC-KS) utilizes pairing-based cryptography and provides keyword search on ciphertext stored in the cloud server in order to facilitate data retrieval without threatening data confidentiality. To validate the scheme workflow, the authors showed a realistic example. The simulation results showed that LDAC-KS improves communication and computation overhead.

Authors in [98] emphasized mutual authentication in Smart City applications (i.e. both sensors and server should be authenticated before exchanging data). The proposed protocol is efficiently adapted to resource-constrained devices that are deployed in Smart City applications. The Smart City system consists of things, intermediate nodes (i.e. routers and gateways), Cloud server, and users. The authors presented a lightweight public key cryptography scheme performed in four phases: system setup, key generation, encryption, and decryption. Then, they detailed the mutual authentication protocol based on the lightweight encryption scheme. Comparing with existing RSA and ECC based protocols, the proposed scheme is more efficient in term of communication cost and security level.

We notice from Table 3 that many distinct solutions are proposed for improving the IoT security in different application domains. However, it is still challenging to develop lightweight security solutions suitable for constrained-resources devices.

6 Discussion and Conclusion

The number of IoT devices is soaring, and the amount of data is increasing as well. This growth is faced with several security issues which should be handled to ensure the evolution of the IoT into a secure infrastructure. Conventional security mechanisms cannot be fully integrated with IoT environments since the IoT devices have inherently limited resources. Therefore, the development of effective security solutions for tiny embedded devices is required. Moreover, the design of intelligent objects should progress toward more autonomy in detecting and recovering from attacks. In a dynamic, heterogeneous, and large-scale environment, adaptive trust models are required to enable devices to recognize trustworthy nodes. Also, an efficient key management should be considered in such networks. To ensure end-to-end security in the context of the IoT, standardized security protocols are highly required.

In this paper, we have reviewed recent related work and their shortcomings. We have performed analysis of the IoT security vulnerabilities and attacks. Then, we have presented a taxonomy of IoT security requirements based on the attacks' purposes. This taxonomy can help developers and researchers in designing new schemes to address security in the context of the IoT. We also have detailed some current security solutions proposed in different IoT application domains. Finally, we conclude that the evolution of the IoT faces many security issues. The major challenge is to develop effective and adaptative secure mechanisms for resource-constrained devices.

References

1. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645.
2. Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. *Journal of Network and Computer Applications*, *42*, 120.
3. Saif, I., Peasley, S., & Perinkolam, A. (2015). Safeguarding the Internet of Things: Being secure, vigilant, and resilient in the connected age. *Deloitte Review*, *17*. https://www2.deloitte.com/insights/us/en/deloitte-review/issue-17/internet-of-things-data-security-and-privacy.html.
4. Vermesan, O., & Friess, P. (2013). *Internet of Things: Converging technologies for smart environments and integrated ecosystems*. Aalborg: River Publishers.
5. Singh, S., & Singh, N. (2015). In *2015 International conference on Green computing and Internet of Things (ICGCIoT)* (pp. 1577–1581). IEEE.
6. Borgohain, T., Kumar, U., & Sanyal, S. (2015). Survey of security and privacy issues of Internet of Things. arXiv preprint arXiv:1501.02211.
7. Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: Perspectives and challenges. *Wireless Networks*, *20*(8), 2481.
8. Cesare, S. (2014). Breaking the security of physical devices. *Presentation at Blackhat*, *14*. http://regmedia.co.uk/2014/08/06/dfgvhbhjkui867ujk5ytghj.pdf.
9. Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015). In *2015 IEEE symposium on computers and communication (ISCC)* (pp. 180–187). IEEE.
10. Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and Internet of Things: A survey. *Future Generation Computer Systems*, *56*, 684.
11. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, *17*(4), 2347.
12. Bormann, C., Castellani, A. P., & Shelby, Z. (2012). Coap: An application protocol for billions of tiny internet nodes. *IEEE Internet Computing*, *16*(2), 62.
13. Rghioui, A., Bouhorma, M., & Benslimane, A. (2013). In *2013 5th International conference on information and communication technology for the Muslim world (ICT4M)* (pp. 1–5). IEEE.
14. Ullah, S., Ali, M., Hussain, A. & Kwak, K. S. (2009). Applications of UWB technology. arXiv preprint arXiv:0911.1681.
15. Madlmayr, G., Langer, J., Kantner, C., & Scharinger, J. (2008). In *Third international conference on availability, reliability and security, 2008. ARES 08* (pp. 642–647). IEEE.
16. Curran, K., Millar, A., & Garvey, C. Mc. (2012). Near field communication. *International Journal of Electrical and Computer Engineering*, *2*(3), 371.
17. Cole, P. H., & Ranasinghe, D. C. (2007). *Networked RFID Systems & lightweight cryptography*. Berlin: Springer.
18. Eisenbarth, T., & Kumar, S. (2007). A survey of lightweight-cryptography implementations. *IEEE Design & Test of Computers*, *24*(6), 522–533.
19. Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2017). A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks*, *4*, 118–137.
20. Mendez, D. M., Papapanagiotou, I., & Yang, B. (2017). Internet of Things: Survey on security and privacy. arXiv preprint arXiv:1707.01879.
21. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of Things Journal*, *4*(5), 1250.

22. Chahid, Y., Benabdellah, M., & Azizi, A. (2017). In *2017 International conference on wireless technologies, embedded and intelligent systems (WITS)* (pp. 1–6). IEEE.
23. Oracevic, A., Dilek, S., & Ozdemir, S. (2017). In *2017 International symposium on networks, computers and communications (ISNCC)* (pp. 1–6). IEEE.
24. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of things security: A survey. *Journal of Network and Computer Applications*, *88*, 10.
25. Razzaq, M. A., Gill, S. H., Qureshi, M. A., & Ullah, S. (2017). Security issues in the Internet of Things (IoT): A comprehensive study. *International Journal of Advanced Computer Science and Applications*, *8*(6), 383.
26. Riahi, A., Natalizio, E., Challal, Y., Mitton, N., & Iera, A. (2014). In *2014 International conference on computing, networking and communications (ICNC)* (pp. 183–188). IEEE.
27. Ronen, E., & Shamir, A. (2016). In *2016 IEEE European symposium on security and privacy (EuroS&P)* (pp. 3–12). IEEE.
28. Zhao, K., & Ge, L. (2013). In *2013 9th International conference on computational intelligence and security (CIS)* (pp. 663–667). IEEE.
29. Perrig, A., Stankovic, J., & Wagner, D. (2004). Security in wireless sensor networks. *Communications of the ACM*, *47*(6), 53.
30. Mo, Y., & Sinopoli, B. (2009). In *47th Annual Allerton conference on communication, control, and computing, 2009. Allerton 2009* (pp. 911–918). IEEE.
31. Soni, V., Modi, P., & Chaudhri, V. (2013). Detecting sinkhole attack in wireless sensor network. *International Journal of Application or Innovation in Engineering & Management*, *2*(2), 29.
32. Lee, P., Clark, A., Bushnell, L., & Poovendran, R. (2014). A passivity framework for modeling and mitigating wormhole attacks on networked control systems. *IEEE Transactions on Automatic Control*, *59*(12), 3224.
33. Yang, X., He, X., Yu, W., Lin, J., Li, R., Yang, Q., et al. (2015). Towards a low-cost remote memory attestation for the smart grid. *Sensors*, *15*(8), 20799.
34. Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C., & Pantziou, G. (2009). A survey on jamming attacks and countermeasures in WSNs. *IEEE Communications Surveys & Tutorials*, *11*(4), 42–56.
35. Ghafir, I., Prenosil, V., Alhejailan, A., & Hammoudeh, M. (2016). In *2016 IEEE 4th international conference on future Internet of Things and cloud (FiCloud)* (pp. 145–149). IEEE.
36. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, *4*(5), 1125.
37. Padhy, R. P., Patra, M. R., & Satapathy, S. C. (2011). Cloud computing: Security issues and research challenges. *International Journal of Computer Science and Information Technology & Security (IJCSITS)*, *1*(2), 136.
38. Nawir, M., Amir, A., Yaakob, N., & Lynn, O. B. (2016). In *2016 3rd International conference on electronic design (ICED)* (pp. 321–326). IEEE.
39. Alsaadi, E., & Tubaishat, A. (2015). Internet of Things: Features, challenges, and vulnerabilities. *International Journal of Advanced Computer Science and Information Technology*, *4*(1), 1.
40. Misra, S., Krishna, P. V., Agarwal, H., Saxena, A., & Obaidat, M. S. (2011). In *2011 International conference on Internet of Things (iThings/CPSCom) and 4th international conference on cyber, physical and social computing* (pp. 114–122). IEEE.
41. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. *Computer Networks*, *57*(10), 2266.
42. Khoo, B. (2011). In *2011 International conference on Internet of Things (iThings/CPSCom) and 4th international conference on cyber, physical and social computing* (pp. 709–712). IEEE.
43. Thakur, B. S., & Chaudhary, S. (2013). Content sniffing attack detection in client and server side: A survey. *International Journal of Advanced Computer Research*, *3*(2), 7.
44. Mitrokotsa, A., Rieback, M. R., & Tanenbaum, A. S. (2010). Classifying rfid attacks and defenses. *Information Systems Frontiers*, *12*(5), 491.
45. Laurie, A. (2007). Practical attacks against RFID. *Network Security*, *2007*(9), 4.
46. Sushma, D. N., & Nandal, V. (2011). Security threats in wireless sensor networks. *IJCSMS International Journal of Computer Science & Management Studies*, *11*(01), 59.
47. Zhang, K., Liang, X., Lu, R., & Shen, X. (2014). Sybil attacks and their defenses in the Internet of Things. *IEEE Internet of Things Journal*, *1*(5), 372.
48. Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94.
49. Zhang, J., Gu, D., Guo, Z., & Zhang, L. (2010). In *2010 3rd International conference on advanced computer theory and engineering (ICACTE)* (Vol. 6, pp. V6–61). IEEE.

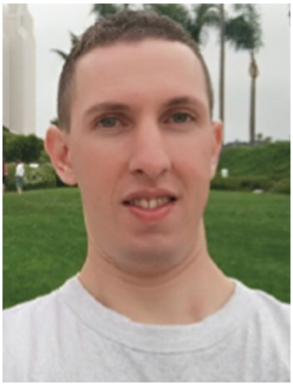
50. Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S. L., Kumar, S. S., & Wehrle, K. (2011). Security challenges in the IP-based Internet of Things. *Wireless Personal Communications*, *61*(3), 527.
51. Hossain, M. M., Fotouhi, M., & Hasan, R. (2015). In *2015 IEEE world congress on services (SERVICES)* (pp. 21–28). IEEE.
52. Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, *10*(7), 1497.
53. Alam, S., Chowdhury, M. M., & Noll, J. (2011). Interoperability of security-enabled Internet of Things. *Wireless Personal Communications*, *61*(3), 567.
54. Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R. (2011). In *2011 2nd International conference on wireless communication, vehicular technology, information theory and aerospace & electronic systems technology (Wireless VITAE)* (pp. 1–5). IEEE.
55. Singh, J., Pasquier, T., Bacon, J., Ko, H., & Eyers, D. (2016). Twenty security considerations for cloud-supported Internet of Things. *IEEE Internet of Things Journal*, *3*(3), 269.
56. Weber, R. H. (2015). Internet of Things: Privacy issues revisited. *Computer Law & Security Review*, *31*(5), 618.
57. Misra, S., Maheswaran, M., & Hashmi, S. (2017). *Security challenges and approaches in Internet of Things*. Berlin: Springer.
58. Sweeney, L. (2002). k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *10*(05), 557.
59. Machanavajjhala, A., Gehrke, J., Kifer, D., & Venkitasubramaniam, M. (2006). In *Proceedings of the 22nd international conference on data engineering, 2006. ICDE'06* (pp. 24–24). IEEE.
60. Li, N., Li, T., & Venkatasubramanian, S. (2007). In *IEEE 23rd international conference on data engineering, 2007. ICDE 2007* (pp. 106–115). IEEE.
61. Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., & Ribagorda, A. (2009). LAMED: A PRNG for EPC class-1 generation-2 RFID specification. *Computer Standards & Interfaces*, *31*(1), 88.
62. Melia-Segui, J., Garcia-Alfaro, J., & Herrera-Joancomarti, J. (2010). In *International conference on financial cryptography and data security* (pp. 34–46). Springer.
63. Mandal, K., Fan, X., & Gong, G. (2013). Warbler: A lightweight pseudorandom number generator for EPC C1 Gen2 passive RFID tags. *International Journal of RFID Security and Cryptography*, *2*, 82.
64. Mace, F., Standaert, F. X., Quisquater, J. J., et al. (2007). In *Proceedings of the third international conference on RFID security-RFIDSec* (pp. 103–114).
65. Gong, Z., Nikova, S., & Law, Y. W. (2011). In *International workshop on radio frequency identification: Security and privacy issues* (pp. 1–18). Springer.
66. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., & Wingers, L. (2015). Simon and speck: Block ciphers for the Internet of Things. *IACR Cryptology ePrint Archive*, *2015*, 585.
67. Hell, M., Johansson, T., & Meier, W. (2007). Grain: A stream cipher for constrained environments. *International Journal of Wireless and Mobile Computing*, *2*(1), 86.
68. David, M., Ranasinghe, D. C., & Larsen, T. (2011). In *2011 IEEE international conference on RFID (RFID)* (pp. 176–183). IEEE.
69. Fan, X., Mandal, K. & Gong, G. (2013). In *International conference on heterogeneous networking for quality, reliability, security and robustness* (pp. 617–632). Springer.
70. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787.
71. Bogdanov, A., Knežević, M., Leander, G., Toz, D., Varıcı, K., & Verbauwhede, I. (2011). In *International workshop on cryptographic hardware and embedded systems* (pp. 312–325). Springer.
72. Berger, T. P., D'Hayer, J., Marquet, K., Minier, M., & Thomas, G. (2012). In *International conference on cryptology in Africa* (pp. 306–323). Springer.
73. Aumasson, J. P., Henzen, L., Meier, W., & Naya-Plasencia, M. (2013). Quark: A lightweight hash. *Journal of cryptology*, *26*(2), 313.
74. Abyaneh, M. R. S. (2012). Security analysis of lightweight schemes for RFID systems, PhD thesis, University of Bergen, Norway.
75. Greenstadt, R., & Beal, J. (2008). In *Proceedings of the 1st ACM workshop on AISec* (pp. 27–30). ACM.
76. Gusmeroli, S., Piccione, S., & Rotondi, D. (2013). A capability-based security approach to manage access control in the Internet of Things. *Mathematical and Computer Modelling*, *58*(5–6), 1189.
77. Liu, J., Xiao, Y., & Chen, C. P. (2012). Internet of Things' authentication and access control. *International Journal of Security and Networks*, *7*(4), 228.

78. Bouij-Pasquier, I., Ouahman, A. A., El Kalam, A. A., & de Montfort, M. O. (2015). In *2015 IEEE/ACS 12th international conference of computer systems and applications (AICCSA)* (pp. 1–8). IEEE.
79. Dennis, J. B., & Van Horn, E. C. (1966). Programming semantics for multiprogrammed computations. *Communications of the ACM*, *9*(3), 143.
80. Mahalle, P. N., Anggorojati, B., Prasad, N. R., Prasad, R., et al. (2013). Identity authentication and capability based access control (iacac) for the Internet of Things. *Journal of Cyber Security and Mobility*, *1*(4), 309.
81. Hernández-Ramos, J. L., Jara, A. J., Marin, L., & Skarmeta, A. F. (2013). Distributed capability-based access control for the Internet of Things. *Journal of Internet Services and Information Security (JISIS)*, *3*(3/4), 1.
82. Mahalle, P. N., Thakre, P. A., Prasad, N. R., & Prasad, R. (2013). In *2013 3rd International conference on wireless communications, vehicular technology, information theory and aerospace & electronic systems (VITAE)* (pp. 1–5). IEEE.
83. Pathan, A. S. K., Lee, H. W., & Hong, C. S. (2006). In *The 8th international conference on advanced communication technology, 2006. ICACT 2006* (Vol. 2, p. 6). IEEE.
84. Oriwoh, E., al Khateeb, H., & Conrad, M. (2016). In *International conference on computing and technology innovation (CTI 2015).*
85. Koblitz, N., Menezes, A., & Vanstone, S. (2000). The state of elliptic curve cryptography. *Designs, Codes and Cryptography*, *19*(2–3), 173.
86. Fan, J., Batina, L., & Verbauwhede, I. (2008). In *International workshop on selected areas in cryptography* (pp. 387–400). Springer.
87. Coetzee, L., & Eksteen, J. (2011). In *IST-Africa conference proceedings, 2011* (pp. 1–9). IEEE.
88. Etalle, S., den Hartog, J., & Marsh, S. (2007). In *Proceedings of the 1st international conference on autonomic computing and communication systems (ICST)* (p. 5). Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering.
89. Kasinathan, P., Pastrone, C., Spirito, M. A., & Vinkovits, M. (2013). In *2013 IEEE 9th international conference on wireless and mobile computing, networking and communications (WiMob)* (pp. 600–607). IEEE.
90. Sheng, Z., Yang, S., Yu, Y., Vasilakos, A., Mccann, J., & Leung, K. (2013). A survey on the IETF protocol suite for the Internet of Things: Standards, challenges, and opportunities. *IEEE Wireless Communications*, *20*(6), 91.
91. Suo, H., Wan, J., Zou, C. & Liu, J. (2012). In *2012 International conference on computer science and electronics engineering (ICCSEE)* (Vol. 3, pp. 648–651). IEEE.
92. Sridhar, S., & Smys, S. (2017). In *2017 International conference on inventive systems and control (ICISC)* (pp. 1–5). IEEE.
93. Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, *56*(6), 34.
94. Song, T., Li, R., Mei, B., Yu, J., Xing, X., & Cheng, X. (2017). A privacy preserving communication protocol for iot applications in smart homes. *IEEE Internet of Things Journal*, *4*(6), 1844.
95. Li, F., Hong, J., & Omala, A. A. (2017). Efficient certificateless access control for industrial Internet of Things. *Future Generation Computer Systems*, *76*, 285.
96. Li, R., Song, T., Capurso, N., Yu, J., Couture, J., & Cheng, X. (2017). IoT applications on secure smart shopping system. *IEEE Internet of Things Journal*, *4*(6), 1945.
97. Yang, Y., Zheng, X., & Tang, C. (2017). Lightweight distributed secure data management system for health Internet of Things. *Journal of Network and Computer Applications*, *89*, 26.
98. Li, N., Liu, D., & Nepal, S. (2017). Lightweight mutual authentication for iot and its applications. *IEEE Transactions on Sustainable Computing*, *2*(4), 359.

Yasmine Harbi obtained her Master diploma in 2017 from Ferhat Abbas University of Setif1, Setif, Algeria. She is currently a Ph.D. student in Computer Science at Ferhat Abbas University of Setif1, Setif, Algeria. She is working on the field of networks and ditributed systems. Her main research interests include wireless sensor networks, fault tolerance, security and privacy in Internet of Things.

Zibouda Aliouat obtained her engineer diploma in 1984 and M.Sc. in 1993 from Constantine University. She received her Ph.D. from Ferhat Abbas University of Setif1, Setif, Algeria. She was an assistant professor at Constantine University from 1985 to 1994. Currently, she is an Associate Professor in Computer Science Department at Ferhat Abbas University of Setif1, Setif, Algeria. Her research interests include computer networks and communication modeling and simulation, wireless sensor networks, fault tolerance of embedded systems and security and privacy in Internet of Things.

Saad Harous obtained his Ph.D. in Computer Science from Case Western Reserve University, Cleveland, OH, USA in 1991. He has more than 25 years of experience in teaching and research in three different countries: USA, Oman and UAE. He is currently an Associate Professor at the College of Information Technology, in the United Arab Emirates University. His teaching interests include programming, data structures, design and analysis of algorithms, operating systems and networks. His research interests include parallel and distributed computing, P2P delivery architectures, wireless networks and the use of computers in education and processing Arabic language. He has published more than 120 journal and conference papers. He is an IEEE senior member.



Abdelhak Bentaleb received the M.S. degree in computing (network and multimedia) from Mohamed El Bachir El Ibrahimi University, Bordj Bou Arreridj, Algeria in 2011. He is currently working towards his Ph.D. degree in computer science at the School of Computing, the National University of Singapore (NUS), Singapore. His research interests include multimedia systems and communication, video streaming architectures, content delivery, distributed computing, computer networks and protocols, wireless communications, and mobile networks.

Allaoua Refoufi obtained his Master diploma in 1980 from University of Colorado at Boulder. He received his Ph.D. from University of Sheffield, Great Britain in 1990. Currently he is an associate professor at Ferhat Abbas University of Setif1, Algeria. His research interests include artificial intelligence, ontology matching algorithms, and big data systems.