Chapter 15
Security Issues of Internet of Things in Health-Care Sector: An Analytical Approach

Pranjal Pandey, Subhash Chandra Pandey and Upendra Kumar

1 Introduction

The Internet as we know is a massive global network that allows people to communicate with each other and it can use homogenous as well as heterogeneous data [1]. The heterogeneous object includes not only communication devices but also diverse physical objects.

The Internet of Things (IoT) is a promising approach and it is pivoted on the interconnectivity of things or devices to each other as well as with users. Indeed, this approach is a cornerstone for the development of smart homes and cities. Perhaps, trustworthiness of any technology is of paramount importance form the viewpoint of users. Further, security and privacy issues play a pivotal role in this pursuit. In spite of vigorous striving of researchers, extensive literature survey revealed the fact that we are still lagging behind trustworthy security and privacy prospects. In IoT, unlike the Internet, things or devices use their computing capabilities together with the network connectivity to sense and collect data from the world around us and share the data across the Internet or cloud and utilize the analyzed and processed data for decision-making. In the world of IoT there are millions of devices connected together. Thereby services should be discoverable by the people by making use of the service discovery mechanism. Nowadays IoT application can be seen in houses, social places,

P. Pandey
Department of Electronics and Communication Engineering, Indraprastha Institute of Information Technology, Delhi, Okhla Industrial Estate, Phase 3, New Delhi, India
e-mail: pranjalpandey200@gmail.com

S. C. Pandey (✉) · U. Kumar
Department of Computer Science and Engineering, Birla Institute of Technology, Mesra, Ranchi (Patna Campus), Patna, Bihar, India
e-mail: s.pandey@bitmesra.ac.in

U. Kumar
e-mail: upendrakumarphdp@gmail.com

O. P. Verma et al. (eds.), *Advancement of Machine Intelligence in Interactive Medical Image Analysis*, Algorithms for Intelligent Systems,
https://doi.org/10.1007/978-981-15-1100-4_15

and industries. For instance, IoT application in houses could be helpful in automatic ordering of online groceries and other home supplies. Cameras together with the sensors, inside the refrigerator, could keep track of the grocery supply and automatic online order is triggered in case of any shortage. Another very interesting example of the smart home IoT application is the self-programmable, Wi-Fi enabled, and sensor-embedded Nest Thermostat which learns what temperature you like and accordingly sets the schedule. Some of the more future prospects of IoT application could be like automatic parking or getting cautionary advice on your phone or wearable device if any physical danger is detected nearby. Addressing these challenges and ensuring security in IoT services and products is very essential. The data and services should be well protected from the cyber-attacks as hacking any single device could provide access to the user data. The information included is personal data of the user like location and time which needs to be secured and privatized. Security services which are needed to be paid are authentication, authorization, confidentiality, and integrity. The application domain of Internet of things could be versatile for example if we are on the way to our holiday vacation, our car could have access to the network and already detect the location of the nearest hotel. There could be many more such applications where in everyday life each object via communication could help do the house chores as well as in business and industrial field. With the excess of IoT devices coming across, the business must develop a universal approach to IoT management, including IoT security, to prevent vulnerabilities of device and related data and services.

With the help of IoT, millions of devices are going to be connected with each other through heterogeneous infrastructures, by avoiding the risk of attack. It requires very less or no human involvement which in turn renders the IoT prone to various attacks such as eavesdropping, man-in-the-middle attack (MMA), and denial of service attack (DSA). In addition, some antagonist devices can have unauthorized access to any physical device in the network. Attacks could easily damage the physical system as well as the connections by compromising the issues of security and privacy pertaining to IoT. Further, the realm of IoT is subject to resource constriction in terms of power, bandwidth, and storage. Therefore, security solutions are needed which will not masticate through the resources of IoT.

Many challenges do stand in the way of security and privacy. Main attacks on IoT system are:

- Spoofing
- False signal injection
- Replay attacks
- Eavesdropping.

The aspects of security are adversely affected by such attacks. Different aspects adversely affected are privacy, reliability, and authenticity. Addressing these challenges and ensuring security in IoT services and products is very essential. The data and services should be well protected from the cyber-attacks as hacking any single device could provide access to the user data. Cryptographic security solutions can gain trust over IoT since the interaction is between human and things and things

and things, much crucial information is shared across the network that could be hacked easily if any of the connected devices is hacked. So, there must be well-defined security architecture deployed with a shared common set of protocols as heterogeneous devices are connected through the IoT network. Many layered architectures are proposed already for example three-layered architecture—perception, network, and application layer. With the impetus of application requirements, large amount of information is being shared among the devices. Moreover, IoT faces many other challenges like scalability, power, bandwidth, security, and privacy. Hence the cryptographic solutions provide the way to utilize the feature of the lightweight symmetric and asymmetric algorithm such that less execution time with optimum energy requirements can be taken care.

In this chapter authors have discussed and analyzed different issues pertaining to the security aspects of IoTs. Further, different measures have been suggested related to security issues of the IoT in different domains. This chapter is organized as follows: Sect. 2 presents the naive information related to IoT. Various security concerns are given in Sect. 3. Security architecture is discussed in Sect. 4. Further, Sect. 5 preludes layered classification. Cryptographic solutions for IoT are given in Sect. 6. Moreover, security **i**ssues of IoT in medical sector are discussed in Sect. 7. Over and above, **s**ecurity analysis of IoT in business sector is delineated in Sect. 8. Finally, chapter is concluded in Sect. 9.

2 Background

The term IoT was coined in Massachusetts Institute of Technology (MIT). As of now, IoT has been the buzzword since the past decades. IoT has versatile importance and applications in different areas, which are very useful for human beings, but IoT being hacked through different ways is also a big challenge for security provider agencies or users. One of the major problems is malware (malicious software) attacks on IoT Systems due to obscurity to patch end devices. Intermediate nodes are used for patching to minimize propagation of malware in IoT system. In [2], authors have compared randomized patching scheme with traffic-aware patching scheme. Since traffic management is one of the major problems of IoT, which is efficiently managed by technique of Operation Research (OR) and system thinking, but system thinking is not a very easy task to implement in IoT for security purposes [3].

The large volume of collected data are mined and used to discover some hidden information to further analyzed data to get certain result in different areas like health care, and business management [4]. In IoT environment, dozens of devices like health-care devices, house controls, house security, and camera are connected with each other. Here, service discovery comes into the picture, which is automatic detection of the devices and services offered by these devices on a computer network. To enhance the capability of IoT, it is necessary for improvement of related technology, methodology, and tools. All these related components will improve living standard of human beings due to diversity of IoT. Diversity of IoT standardized

the lifestyle in different fields like development of agriculture, supply chain management system, work culture of Industry, caring in health, development of smart cities, transportation, entertainment, etc. [5]. In order to capture the full potential use of service discovery, there are many protocols like BLE (Bluetooth Low Energy), Apple Airdrop, and Multicast DNS. In order to secure the quality of services through traffic measurement, it is necessary to improve network performance through simulation for machine type communication [6]. IoT covers large domains to deliver services for smart manufacturing, environmental monitoring, and health services. It also improves quality of life and productivity of humans [7].

Security and privacy were the most concerning parts for the IoT application facing enormous challenges. IoT is extending the frontier of connectivity beyond laptops and smartphones to smart homes, wearable, smart city, connected car, connected health, and many more. A predator–prey model can help to understand the security threats of wireless nano-sensor network (WNSN) which is made of nano-IoT [8]. Inclusion of active mode and sleep mode of sensor nodes makes this work interesting.

It is not a very easy task to connect many devices with IoT, but researchers have taken it as a challenging task for future IoT. Moreover, different models are also proposed to present IoT ecosystem [9]. Such type of network systems will require massive storage device to maintain the cloud servers. In existing scenario, future of IoT greatly depends on decentralization of IoT networks [10]. The various technological challenges which need to be addressed are connectivity, security, compatibility, standards, intelligent analysis, and actions. However, deploying utmost security in all IoT devices is not feasible. Different security solutions have been architectured for homogeneity of network. Another challenge arises due to the risks involved with mission-critical operations in open and un-trusted environments [11].

3 IoT Security Concerns

Any object connected to the Internet is bound for security threats. The new vulnerability emerges and software securities degrade over time. By looking at eternally changing threat landscape from cyber espionage to phishing and from malware to ransomware, we can see most of the attacks are targeted on data. With the advent of IoT, we see more and more connected devices impacting our everyday life. By 2032 it is predicted that every personality will be connected to average 3000–5000 devices. This leads to immense security challenge for all IoT segments [12]. Adoption of ever-changing technology also opens up new avenues for attackers to target and abuse IoT. Perhaps, security architecture is not standardized and varies from vendors to vendors. Keeping different IoT insecurities, security implementation, and protection architecture, in general contain three different levels [13]:

a. Device security (Perception layer)—This is device-level protection and deals mostly with devices, mobile app, and web app integrity. IoT security threat at this level is physical threat which attacks the physical devices.

b. Communication securities (Network and transport layer)—Used for network and communication channel protection.
c. Cloud security (Application layer)—Cloud services particularly vulnerable to exploits, such as SQL injection flaws, will likely be targeted first. Cloud security will insure data protection and will protect data leakage.

3.1 Basics and Related Definitions

Perhaps, prior to dealing with deep insight of IoT, it would be incisive to prelude basic terminologies and definitions to make the further discussions explicit. Following are the terms often used while discussing the IoT:

- IoT
- Big Data
- Cloud Server
- Cloud Computing

IoT is considered as entire things capable to transmit or receive information and can have the efficacy of mutual interaction with each other. Indeed, this realm is moderately pervasive in different walks of life. The salient feature of IoT network can be precisely enumerated as:

- Ability to have data accumulation
- Data Processing
- Data Transmission
- Ability to analyze the entire network component

Researchers are visualizing that in the recent future the IoT will control the world by physical things that would be connected together through an infrastructure of its own [14]. Precisely, we can percept IoT as a gigantic network which encompasses an enormous group of things, sensors, and smart devices [15]. However, sensors are the prevailing component of this network. Other components of this network can be briefly enumerated as:

- RFID
- Smart card
- Smartphone
- Computers to share the necessary information.

Further, there is no explicit definition for the term big data [16]. However, the term big data entails a substantially large volume of data [17]. Different definitions observed through the literature survey unveil the fact that there are varying definitions of big data and is mainly a function of intent and research field. It is also pertinent to mention that the rate of data produced is not a fixed quantity in big data. However, few well known big data generators are YouTube, Facebook, and Twitter [18]. Moreover, wireless sensor networks are also considered as big data generators [19, 20].

It is the researcher's prediction that in the coming future IoT network will have maximum number of shared documents. The IoT network consists of an extremely powerful server to process the information. The cloud server elicits the information from distinct avenues such as from sensors, RFID, and other smart devices. Subsequently, this information is stored in memory [21]. The industry is considered as the genesis of cloud computing such as Google and Amazon [15]. The cloud server is of paramount importance in IoT network. It is due to the fact that IoT network consists of ordinary devices which are not able to store and process the big data.

It is an important issue to consider the trade-off between the big data and IoT. As stated above years ago Facebook was visualized as the gigantic creator of big data. However, in future IoT will undoubtedly be the greatest information exchanging network. Perhaps, in near future major big cities of the world will be transformed into large-scale smart cities [22]. It is worthy to mention that in fourth industrial revolution the apex use of IoT is observed. Moreover, the concomitant use of sensor which is an indispensable component of IoT also begun to augment [23]. Accumulation of environmental information, GIS through wireless sensors also renders the relationship between IoT and big data [24]. In [17], interdependencies between big data and IoT have been discussed with deep insight.

3.2 Key Security Issues

Social media is constantly reflecting the information sharing in different domains which in turn is increasing the pervasive demand of IoT. Further, malevolent and deceitful individuals are also increasing to deceive genuine users. The security of the individual's privacy is of utmost importance. Therefore, in order to save the privacy of innocent users and things some security measures are of prime concern [25–27]. Two substantial components in this pursuit are given below.

- Privacy
- Security

It is of profound interest to prevent the accessibility of information of one user by others [28]. In [29], it has been mentioned that the privacy information can subsequently be categorized in three streams. These are

- Infrastructure security
- Information security
- Information management

Further, there must be provision for each user which can be individual in devices to provide access of its information to others. However, there must be provision to inhibit the access and stop the privacy. It is a strenuous task to provide security while there is a huge volume and velocity of the data. Indeed, plenty of uncertainties subsist on data and information security. Researchers are persistently striving in this pursuit. But, big data security is still murkier and a matter of investigation. However,

to prevent the users against these attacks is an arduous and challenging task. Perhaps, the growing technological advancement will resolve this issue soon [25]. Moreover, security threats entail sub-elements such as [29]:

- Denial of service (DoS)
- Functionalities of encryption
- Access control.

3.3 Features of Big Data

In this section, authors will prelude important features of big data as it is the most indispensable component for providing security. It is also important to mention that authors have considered mainly the current challenges [17, 25, 30–34]. Some important features of big data are enumerated in Table 1.

4 Security Architecture in IoT

IoT network architecture is scalable to manage the surge of devices and will circumscribe a vast range of technologies [35]. Architecture could be delineated as a simple skeleton for the network characteristics and pragmatic organization and composition. Different communication models often used are Thing to Application server and Thing to Human or Thing to Thing communication [36]. IoT architecture will have evolutionary growth and several architecture models which are currently under development like M2M (Machine to Machine) model from ETSI (European Telecommunications Standards Institute), ITU-T (International Telecommunication Union) model should be factored into future developments [37]. Further, it can be divided into four levels as given below.

- Perceptual Layer
- Network Layer
- Support Layer
- Application Layer

The first layer, i.e., the perceptual layer gathers all information like RFID [38] and all kinds of sensor information. Information could be object properties, environmental condition, etc. Security problems in this layer include the attacks from external networks such as denial of services. The functioning of second layer, i.e., network layer is to perform secure communication of the information from the first layer as well as the initial information processing. Security in network layer of IoT is very important. Since threats like MMA can pose danger to security. The support layer is the third layer and it is helpful in setting up the platform for the application layer. This layer does the intelligent processing of massive information. Finally, the

Table 1 Important features of big data

Serial number	Features	Descriptions
1	Volume	• Substantial challenge in BD • Not possible to define the limitations for the big data
2	Velocity	• Velocity is often fast in case of big data
3	Variability	• In general, different sort of data is transmitted in the case of big data
4	Veracity	• The data structure is substantially complex in big data • Difficult to establish confidence
5	Visualization	• Required lucid and adequate information • Key information must be available from each sender
6	Value	• Storage and maintenance of the value of data is required
7	Data acquisition	• Accumulation and storage of data received from different sources are required • Security of this accumulated data is of paramount importance
8	Data mining and cleansing	• It is an indispensable challenging task
9	Data aggregation and integration	• It is an indispensable challenging task
10	Complexity	• Complexity increases with volume • Increased data complexity • Increased computational complexity • Increased system complexity
11	Data analysis and modeling	• Required segregation of information • Fetching of data lost
12	Data interpretation	• Required for decision-making process
13	Privacy	• Most challenging task
14	Security	• Required to maintain the users' privacy and prevention from malware
15	Data governance	• With the increase of big data, companies and organizations need more thrust on data governance
16	Data and information sharing	• Coordination of information sharing is required by all organization
17	Cost	• It increases with demand
18	Data ownership	• Ownership is an indispensable parameter

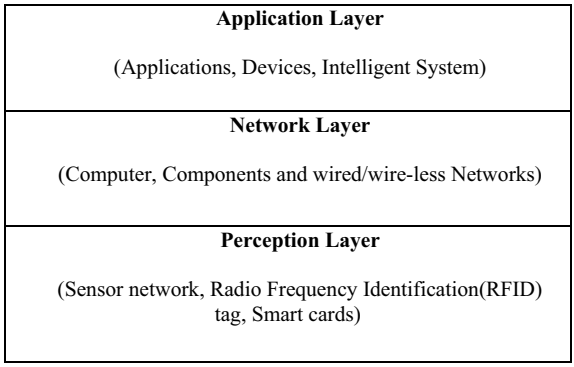

Fig. 1 Different layers in three-layered architecture

uppermost layer is application layer. This layer caters to the users' need. Moreover, sharing of the data is the major characteristic of this layer and thus poses serious concerns for the security. Advantages and risks are discussed in [36]. The schematic representation of different layers is shown in Fig. 1.

4.1 Security Issues in Perception Layer

It is the lowest layer of the IoT architecture. The functionality of this layer is to collect information. This is done by various devices like smart cards, RFID tags, and sensor networks. This layer has ability to get the information. The security concerns in this layer lie in the fact that IoT cannot provide security to the sensing devices and information. The reason includes limited energy, fragile security capability of the sensing devices. The RFID system in this layer has security issues such as information leakage, man-in-the-middle attacks, tampering, cloning attacks, and information tracking. Furthermore, security problems faced by perception layers are congestion attack, Denial of service attacks, node replication attack, capture gateway node, and forward attack. Security issues for devices in this layer can be categorized as (a) Terminal security issue and (b) Sensor network security issue.

4.1.1 Terminal Security Issue

For collecting large amounts of real-time information, perception layer needs a lot of terminals to present this information to the user. This process requires an authentication and integrity of data to be maintained. Here, exchange of information is done through RFID technology using RFID tags, which requires no human intervention. The RFID tags are vulnerable to various attacks such as man-in-the-middle or sniffing, power analysis, viruses, cloning, and many more. At this time RFID tags do not have enough memory to store the virus, but in future the virus could be a great

threat to the system. Virus programmed on the chip by the unknown source and when read, virus can transfer from the tag to the reader and then to the company's network bringing down every connected computer, RFID components, and networks. Four common types of attacks in terminal security are:

a. Unauthorized tag disabling: In these types of attacks RFID tags will become incapable temporarily or permanently. In this the attacker manipulates the behavior of the tag which can be done if one is very far away.
b. Unauthorized tag cloning: It cracks up the integrity of the information. The hacker captures the tag's identification information through the manipulation of the tags. Once the identification information of the tag is leaked, this can be used by the hacker to bypass simulated protection and plan for the further theft scheme.
c. Unauthorized tag tracking: This is a privacy attack. The hacker can trace tags by using illegitimate RFID readers. Using which, one can capture sensitive information, for instance a person's address, etc. This type of attack, management could have planned to trace their employees. Another example could be of a customer buying a product having RFID tag which guarantees them no confidentiality and thus endangers their privacy.
d. Replay attacks: This is also an eavesdropping attack. The hacker uses an illegitimate reader to imitate a tag by using a tag's response. This occurs when one side of the communication is obstructed or cut-off recorded and replayed at the later time to the receiving device in order to gain information or access.

4.1.2 Sensor Network Security Issue

There are many security concerns in sensor network. Perhaps, security need in WSN is of utmost concern and security of sensor network is substantially different from conventional network because of mobility, heterogeneity, and cost. Conventional protocols of security cannot be used in WSN. However, many innovative protocols have been designed in the recent past which visualizes the aspect of the WSN [35].

4.2 Security Issue in Network Layer

IoT is deployed in open and physically insecure with the environment which is open for attack. The layer chiefly includes computers, wired or wireless network, and also entails security issues. Further, the layer faces security issues like confidentiality, illegal access, data eavesdropping, DoS attacks, man-in-the-middle attack, virus attack, and so on. A large number of devices in this layer collect data of different formats with information having massive, multisource, and heterogeneous characteristics [35]. Transferring of large data between these nodes encounters the security issue like network congestion, thus giving way to attacks. The attacks taking place in network layer are:

a. Selective Forwarding—This attack includes a compromised node or malicious node taken over by the attacker which may send message to the incorrect pathway [39]
b. HELLO flood attack—The adversary node, which is not a legal node in the system, floods the hello request to any legitimate node. This creates congestion in the traffic by sending a useless message. The current solution of the hello flood attack is cryptographic solution which has high computational complexity [39].
c. The wormhole attack—In simple words, it's the rearrangement of the bits.
d. Sybil attack—This attack aims at fault-tolerant schemes, such as multiple routing, distributed storage, and topology maintenance. The solution to this attack which would prevent any stranger to start a Sybil attack could be Authentication and Encryption techniques.
e. Acknowledgment spoofing—In Acknowledgement flooding attack, an adversary node spoofs the acknowledgements updating the wrong information to the destined neighboring node. Acknowledgement is needed in times when routing algorithm is used.
f. Sinkhole attack—Makes selective forwarding extremely uncomplicated.

4.3 Security Issue in Application Layer

Application layer provides authenticity, integrity, and confidentiality of data. The security concerns in this layer include tampering and eavesdropping. Application layer carries out the task of traffic management and data management with the help of applications software. These attacks target the application layer to rupture the genuine service request traffic and inundate the service which ultimately creates denial of service.

5 Layered Classification

There are on the whole two categories of layered classification of attacks, which are:

- Layered classification of attacks on RFID
- Layered classification of attacks on the WSN
- Layers used for security solution of IoT

The wireless medium used in RFID network has drawbacks since it leaves the system vulnerable to attacks. These attacks are classified based on the layers in which it could be performed, which is shown in Fig. 2a. The figure classifies the RFID network attacks segregating the attacks which could be deployed to physical layer as well as the multilayer, which affects more than one layer. Understanding of security architecture gives the attacker advantage to attack a particular layer. Amongst

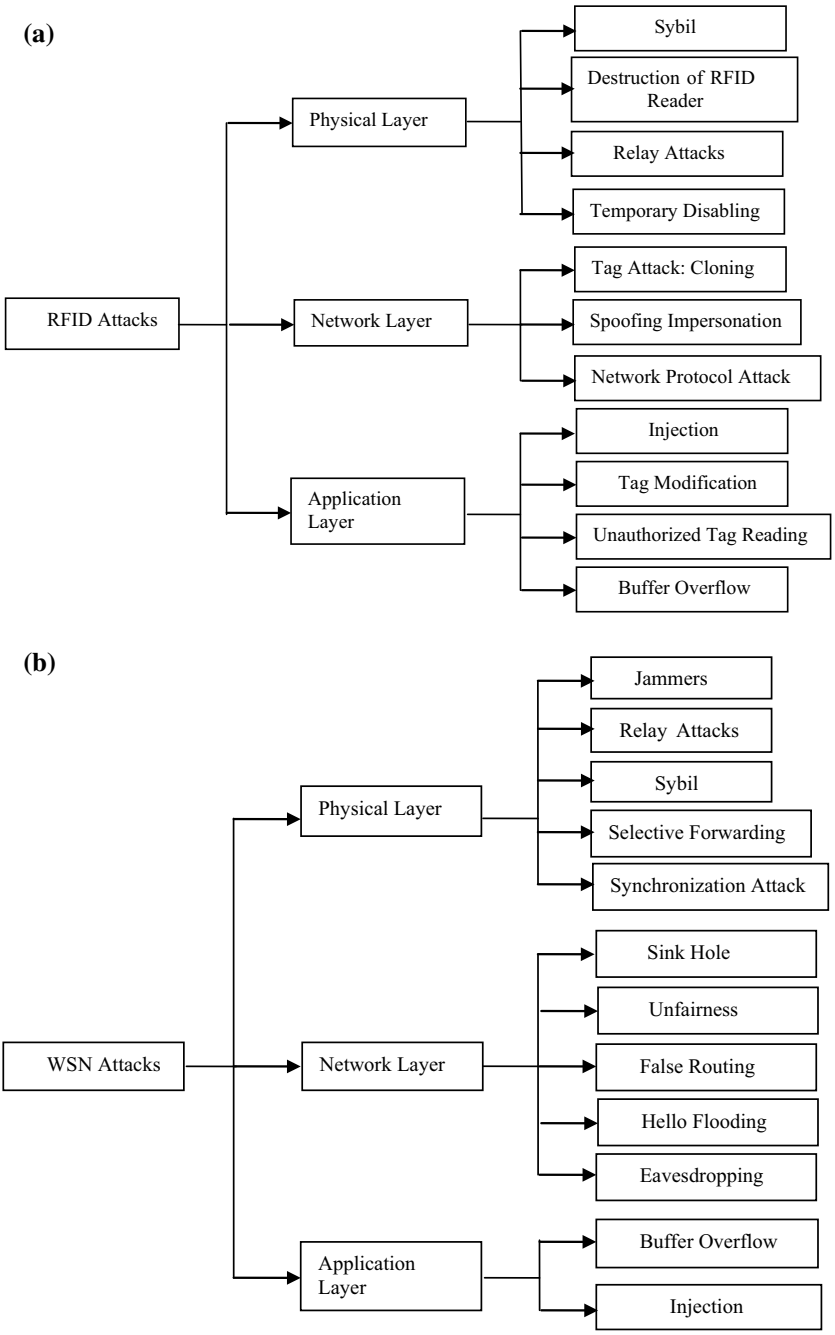

Fig. 2 **a** layered classification of RFID attacks, **b** layered classification of WSN attacks

various other attacks, Sybil attack, replay attack, destruction of RFID readers, temporarily disabling passive interference, active jamming, etc. could be said to have security concerns that are faced by the physical layer. Likewise, on network layer we could find attacks such as cloning, spoofing, eavesdropping, etc. Attacks which are viewed on this layer are injection, buffer overflows, unauthorized tag reading, and tag modification.

There are several attacks possible in WSN (Wireless Sensor Network) and are classified here in Fig. 2b. It depends upon which layer the attacks happen. Classifications of attack on the layer basis helps locate, identify, and mitigate the vulnerabilities due to attack and in many cases prevent these attacks. The intention of attacker in WSN layer is to either jeopardize the benefit of WSN or eavesdrop the network. There are many tools and techniques to deal with attacks in WSN security attacks.

CISCO has claimed that the IoT needs different sorts of network models for communication and processing. A seven layers model is proposed by CISCO. This model of seven layers mainly aims to secure each device and system, and every process at each level. It also provides secure communication between each level [40]. These seven layers are illustrated in Fig. 3.

6 Cryptographic Solutions for IoT

Cryptography involves creating written or generated codes that secure the information. Unauthorized readers cannot access the information since cryptography converts the data into a format that is only readable by the authorized users [40]. Cryptography can be divided into three main functions:

- Confidentiality
- Integrity
- Authentication

Confidentiality implicates that only the sender or receiver can access the data or information. Integrity does not permit an intruder to access the data during the process of transmission. It implicates the identity verification of the sender by the receiver.

6.1 Symmetric Lightweight Algorithm

These algorithms are mainly used for confidentiality purposes [12]. Advanced encryption standard (AES) is an example of this category. It is used to encrypt data and protect it against the unauthorized access. It is originally introduced by the American Institute of Standards and Technology. The cryptographic process key of varied length is used—AES-128, AES-192, or A256 depending on the length. This type of encryption of any type of data is particularly safe and effective and is

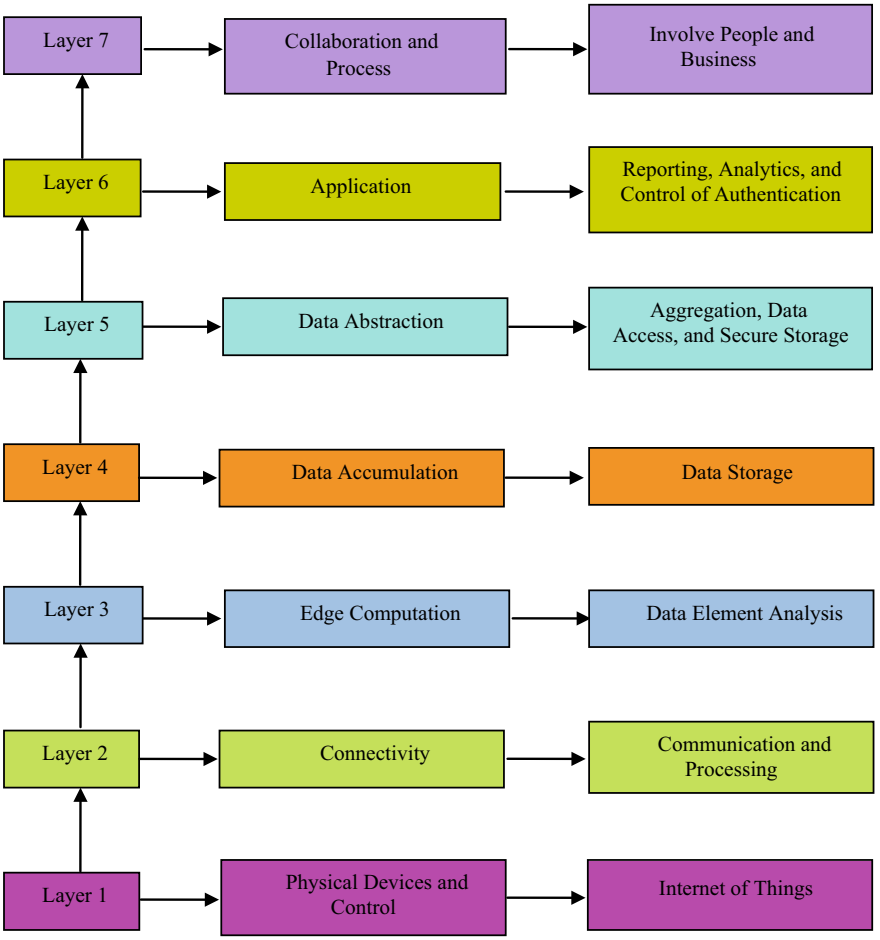

Fig. 3 Illustration of seven layers

used in various protocols and transmission technology for instance WPA2 protection of Wi-Fi networks utilizes the Advanced Encryption Standard. Today, AES is integrated into hardware of many devices to give more effective and rapid encryption and decryption than software solutions. AES is more popular due to the advantage it provides. It is freely usable, no license fees or patent restrictions.

Moreover, it has low storage, and encryption algorithm is simple to code and implement. AES is prone to the attack of MMA.

- High Security and Lightweight (HIGHT)—During Encryption and Decryption phase its keys are generated. Parallel implementation of HIGHT requires less power, fewer lines of code, and a relatively faster and efficient Radio Frequency Identification System.

- Tiny Encryption Algorithm (TEA)—This algorithm works on a constrained environment and uncomplicated. TEA is very less complex and uses basic operations like addition, shifting, and XOR. In [41], space requirement for this algorithm is given.
- PRESENT—It is ultra-lightweight algorithmic solutions. It is vulnerable to differential attack on 26 out of 31 rounds.
- RC5—RC5 is a fast symmetric block cipher suitable for hardware and software implementations. It is well known for its simplicity.

6.2 Asymmetric Lightweight Algorithm

- RSA—This algorithm basically generates a public and private key pair. Further, the public key is made open to everyone where on the other hand the private key is made secure.
- Elliptic Curve Cryptography (ECC). It is discovered in 1985.

6.3 Protocols for IoT Security

There are some essential protocols to secure IoT. These protocols are applicable to execute both symmetric as well as asymmetric cryptographic algorithms.

- HTTP: Hyper Text Transfer Protocol is a keystone of client server-based protocol for the Internet, which is used only in the client side of IoT to initiate connection but not to receive connection request.
- XMPP: Extensible Messaging and Presence Protocol defines a novel concept in IoT. It is especially applicable for voice and video calls as well as strengthening in the sense of addressing security and scalability of IoT systems.
- CoAP: It is applicable to define miserable nodes and is also capable to manipulate existing recourse with the help of interfaces. Some functions of TCP are also replicated in it, although it uses user datagram protocol.
- MQTT: Message Queue Telemetry Transport has been designed and developed for unreliable network system having low bandwidth. It controls the overall network from backend server.
- AMQP: Advance Message Queuing Protocol is applicable for queuing and routing in IoT-based system for point to point communication and security.

7 Security Issues of IoT in Medical Sector

In [42], it has been mentioned that by 2016 the approximate market of medical-related devices will be $5 billion. However, in [43], it has been given that the bulk of medical organizations are not concentrating properly on the issue pertaining to protect patient data. It is reflected in the study of [44] that the plethora of cases have occurred regarding the security in the domain of health care. Perhaps, due to the lack of effective security measure the health data is an enticing and tempting object for a malicious doer. Nowadays, smartphones equipped with sensors and other wearable devices are being used to collect the biometric data of the patients. Generally, these are connected with the apps for processing and interpreting the data and signals. The functionalities of these apps are often broadened by communicating the data to the cloud and this phenomenon required complex algorithms. The realm of security in this prospect encompasses three main ingredients. These are:

1. Confidentiality
2. Genuine use of information
3. Legal issues.

Further, three points of vulnerability pertaining to security are:

1. Devices
2. Data transmission
3. Cloud storage

It is pertinent to mention that the susceptibility of data theft from devices is less. However, one cannot defy from the chances of data theft from devices by using malware. Physical devices are also prone to be stolen or lost. Further, protection does not entail wearable sensors. But, there is provision of configuration of mobile by users. However, data can be hacked using different malware during the phenomenon of data transmission. Indeed, efficient encryption approach and method of authentication is needed to avoid the hacking of data. But there are certain pitfalls pertaining to encryption and authentication which need to be resolved. These are the reduction in the data transfer rate, difficulty of pragmatic implementation, and high energy consumption. Finally, the data is saved in the database of cloud computing architecture. However, this service is imparted by different third party vendors and thus there are more chances of attacks. Further, these databases are accessible to the Internet network so that data can be fetched from the users. It further augments the chances of attacks. In order to resolve these issues multifaceted authenticity, some access controlling technique, and complex password is needed which in turn render the system more complicated to use.

7.1 An IoT Architecture for Medical Sector

In [45], architecture for the data accumulation is proposed which needs scalable data storage devices with high performance computing (HPC) infrastructure so that efficient storage, processing and sharing of sensor data pertaining to health can take place. In this proposed architecture, logical solution monitoring is given. The solution thus obtained encompasses many parameters such as noninvasive sensors. The characteristics of these sensors are to permit the processing of voluminous data. Moreover, the solution also renders the searching and retrieval of health-related information. Figure 4 shows the general architecture for the purposes of activity monitoring based on the features given above. Furthermore, the elements of Fig. 1 are developed for the project given in [46]. This architecture lets to register the observation of persistent and nonpersistent patients and healthy people as well. Moreover, this architecture also permits the mutual communication between the family and hospitals via pragmatic application of cloud computing, big data, IoT. In this architecture IoT plays pivotal roles. In addition, this architecture incorporates the following components:

- Smart mobile phone.
- Cloud-based infrastructure.
- Analytic module.
- Access element.
- Interoperability and messaging platform.
- Website platform.

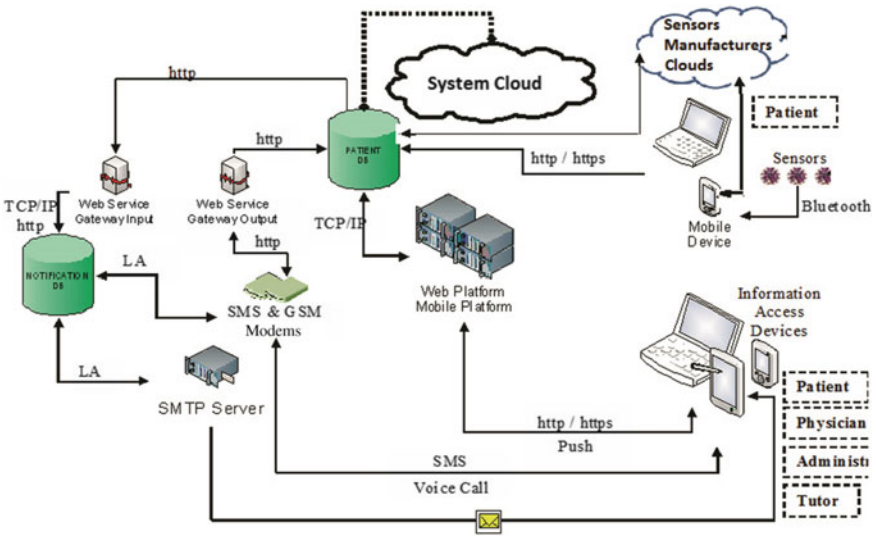

Fig. 4 Proposed architecture for patients monitoring [48]

The first element accepts the data from the sensors. The second element is required for the purposes of data storage. The third element is the need for sending the alarms to the patient and hospital. The fourth element is required to access different sensors of cloud manufacturers. Further, the fifth element is required for delivery of information for everyone involved in the system. Finally, the last element is required to permit the access of related information of the patient from the computer and from the mobile as well.

8 Security Analysis of IoT in Business Sector

IoT strategy implemented in the business sector influences the end users and is mainly designed on the basis of devices. Moreover, security features are included in an ad hoc fashion and thrust is given on threats. However, threats associated at hardware level are always there [47]. Indeed, hardware-level security issues are of the prime concern while designing the IoT architecture to cater to the need of the business sector.

8.1 Case Study

Authors are including include home automation system (Haier's system) as a case study in this chapter. The said system is treated as a smart system for controlling and reading the information obtained from different sensors installed at various places in the user's home. Different information obtained from these sensors is given below.

- Leakage of water.
- Smoke detecting sensor.
- Sensor to check the opening and closing position of the door.
- A remotely situated power switch.

Different sensors are linked by a specific protocol known as "Zigbee". The basic utility of this system is to observe the home and to receive the warning alarm on the basis of information achieved by the sensors. First of all, users are required to install a mobile app prepared by the home care system of producer. Further, this home system is linked to users' network by ethernet connectivity. Furthermore, the mobile is also linked to the same local network. Subsequently, the mobile app is opened and an account is created through the cloud service of the producer. This will enable the users to see their sensor data while the users are away from the local network.

The first phase of analysis is to analyze the hardware elements of this home security system. The processor used in this home security system supports the Linux and Android OS. The printed circuit board hardware platform and daughter board of this system is shown in Fig. 5a and b, respectively. The system also provides the capability of reading the serial data as well as the startup. At the commencement of

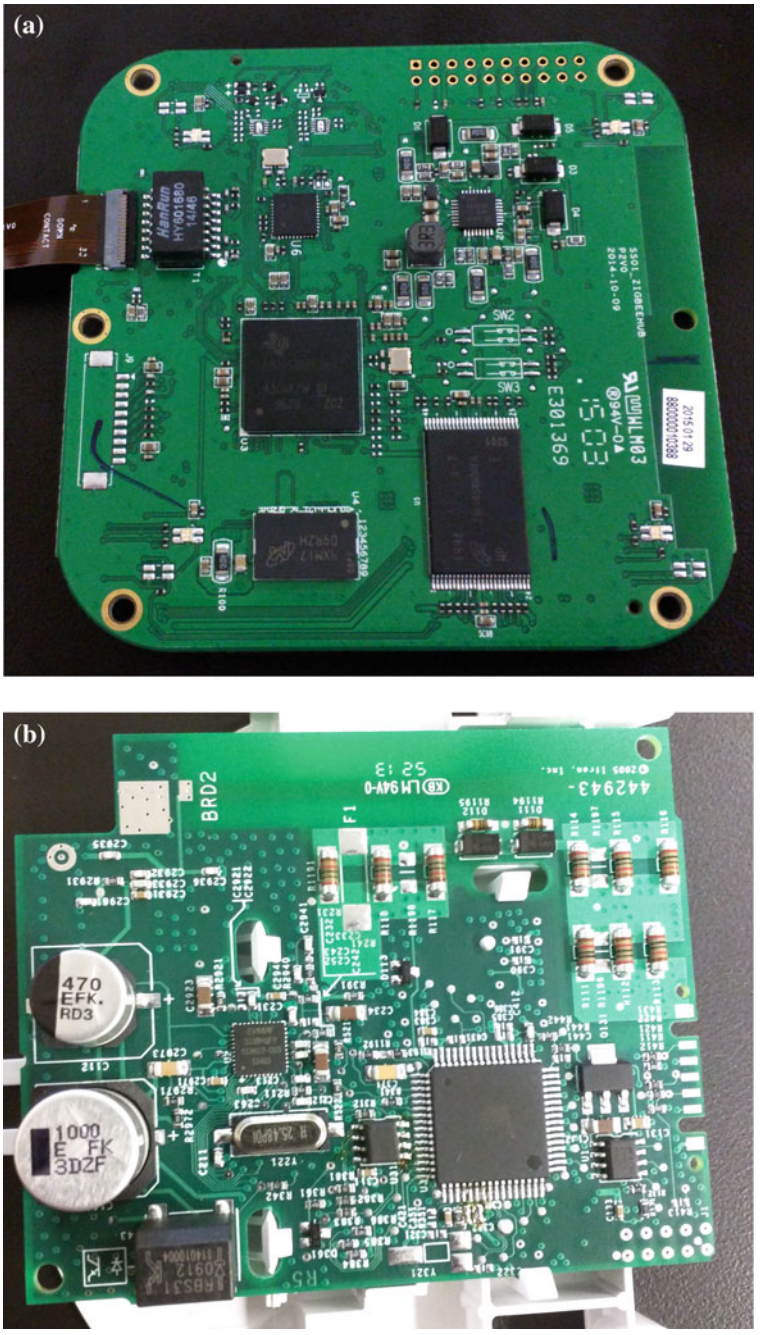

Fig. 5 **a** Smart care hardware platform [45], **b** smart meter CL200 daughterboard [45]

the booting the system displays “whether user wants to terminate the usual booting progression?” Moreover, at the termination of this phenomenon the user is allowed to go into a U-booting shell. This shell permits the modification of peculiar parameters of the system pertaining to boot. However, it is still possible that hackers can fetch low-level information from this system after modification in starting shell.

Subsequently after the modification of parameters booting process is initialized. After the completion of the booting process, the user enters into “rudimentary shell”.

After observing the output of the system, let us suppose that the device is working on Linux. Further, in Linux environment it is indispensable to be acquainted with the type of permission users have, administration id displayed to the users that they were on the source account of the apparatus. Further, the busy box utility delineates that the user is able to run a telnet server. Further, it will permit the “TFTP” file transfer and “wget” enables the system to get the files from web. The root shell also provides the efficacy to observe the password hashes on the system.

The password can implement up to eight characters. It is pertinent to mention that getting the root password requires cracking of password hash which requires a dictionary attack. In this attack, each included password is hashed and thereafter checked for the hash under consideration. Matching of hash will provide the password otherwise checking will be continued. In addition, brute force attack is another option. However, time complexity of this approach is more.

Often, excellent hardware performance coupled with parallel processing is pragmatically used for optimizing the cracking phenomenon. In this case study, two “AMD R9290” graphics cards are used for speeding up the process. Further, it has been observed that almost 5 h is needed to obtain the root password. However, if root password is already known moving to the other layer of attack is the next disposition.

The next attack of interest to be accomplished is the remote attack on the basis of network. First of all, in this attack network scanning is performed. The network scanning enables the user to recognize “whether device possess a telnet server or not?” Next, after the linking of the device with telnet, login prompt is displayed. Further, with the help of root records, root shell can be obtained over a local network. Furthermore, type of traffic generation is observed. Moreover, in order to analyze the type of traffic generation “man-in-the-middle” is done.

Computer is required as the gateway of the system’s network. Now, the internet access can be performed via the gateway. In the next step, packet sniffing is performed to observe the type of traffic the device is generating. It is worthy to mention that the firmware is being fetched on plaintext linking. Now, the updates can be fetched with the help of “wget” and file can be analyzed on it which in turn imparts the “ZIP archive”. Subsequently, this archive is unzipped and lets the observation of main binary of this system with hash script needed for the device updating. On the basis of this initialized script, the device will re-setup from its own accord and further the main binary is executed. After getting this information, next phase in this analysis is to observe the way device is tackling the firmware. In this phenomenon reverse engineering and binary is needed.

Further, software is used for the binary analysis. This analysis renders the binary searching which in turn displays the way of updates handling. “MQTT” protocol

is used for secured communication through the encrypted channel. Moreover, it performs as a publisher and backpropagates the sensors' related information to producer's server.

9 Conclusions

In this chapter, authors prelude an analytic view of existing key security issues pertaining to IoT security and several protocols have been reviewed. The latest research has demonstrated that IoT has huge potential for serving the industry with a titanic impact on the world, but it also poses a great threat to privacy and security. In this chapter, preoccupied architecture which connects physical world to the network has been discussed. IoT being the upcoming technology isstill in its early phase of development. Indeed, it seems that it will encompass a wide spectrum in the future. Many subdivisions of smart city, connected industry, smart energy, connected car, smart retail, and smart agriculture are controlled by IoT using RFID system. Numerous energy-constrained devices and sensors are being continuously communicating with each other via IoT technology but the security of which must not be compromised.

IoT cannot be used if it's not safe, therefore security attacks and countermeasures have been mentioned in this chapter. Various security challenges are laid before and to prevent quite a lot of attacks, one needs lightweight cryptographic security solutions, which adds on to high computational complexity. The implementations show promising results making the algorithm suitable to be adopted in IoT applications. However, it is intuitive to ponder that there is no unique solution which can cater to all the needs. Moreover, the IoT solution varies from domain to domain. Therefore, it is of paramount importance to comprehend all the necessities of an IoT implementation prior to designing an IoT solution. Designing a viable and pragmatic security solution in the realm of IoT can be considered as a future research endeavor.

References

1. Evans D (2011) The internet of things: how the next evolution of the internet is changing everything. CISCO 1–11
2. Cheng S-M, Chen P-Y, Lin CC, Hsiao H-C (2017) Traffic-aware patching for cyber security in mobile IoT. IEEE Commun Mag 29–35
3. Ryan PJ, Watson RB (2017) Research challenges for internet of things. System (MDPI) 1–32
4. Ammar M, Russello G, Crispo B (2018) Internet of things: a survey on the security of IoT frameworks. J Inf Secur Appl (Elsevier) 8–27
5. Ray PP (2018) A survey on internet of things architectures. J King of Saud Univ Comput Inf Sci (Elsevier) 291–319
6. Al-Shammari BKJ, Al-Aboody N, Al-Raweshidy HS (2018) IoT traffic management and integration in the QoS supported network. IEEE Internet Things J 352–370
7. Bertino E, Choo K-KR, Georgakopolous D, Nepal S (2016) Internet of things: smart and secure service delivery. ACM Trans Internet Technol 16(4), Article 22

8. Keshri AK, Mishra BK, Mallick DK (2018) A predator–prey model on the attacking behaviour of malicious objects in wireless nanosensor networks. Nano Commun Netw (Elsevier) 15:1–16
9. Al-Karaki JN, Kamal AE (2004) Routing techniques in wireless sensors networks: a survey. IEEE Wirel Sens Netw 11(6):6–28
10. Xiwen S (2012) Study on security issue of internet of things based on RFID. In: Fourth international conference on computational and information sciences, pp 566–569
11. Wood A, Fang L, Stankovic J, He T (2006) SIGF: a family of configurable secure routing protocols for wireless sensor networks. ACM, SASN, Alexandria, Virginia, USA, pp 1–14
12. Lu T, Wu M, Ling F, Sun J, Duh HY (2010) Research on the architecture of internet of things. In: 3rd international conference on advanced computer theory and engineering, pp 484–487
13. Batra I, Luhach AK (2016) Analysis of lightweight cryptographic solutions for internet of things. Indian J Sci Technol 1–7
14. Rahman AFA, Daud M, Mohamad MZ (2016) Securing sensor to cloud ecosystem using internet of things (IoT) security framework. In: Proceedings of the international conference on internet of things and cloud computing. ACM
15. Hashem IAT et al (2015) The rise of "big data" on cloud computing: review and open research issues. Inf Syst 47:98–115
16. Perera C, Ranjan R, Wang L (2015) Big data privacy in internet of things era. Internet Things (Mag) 32–39
17. Chen CP, Zhang C-Y (2014) Data-intensive applications, challenges, techniques and technologies: a survey on big data. Inf Sci 275:314–347
18. Khan N et al (2014) Big data: survey, technologies, opportunities, and challenges. Sci World J
19. Ding X, Tian Y, Yu Y (2016) A real-time big data gathering algorithm based on indoor wireless sensor networks for risk analysis of industrial operations. IEEE Trans Industr Inf 12(3):1232–1242
20. Kang Y-S et al (2016) MongoDB-based repository design for IoT generated RFID/sensor big data. IEEE Sens J 16(2):485–497
21. Cai H et al (2017) IoT-based big data storage systems in cloud computing: perspectives and challenges. IEEE Internet Things J 4(1):75–87
22. Sun Y et al (2016) Internet of things and big data analytics for smart and connected communities. IEEE Access 4:766–773
23. Khan M et al (2017) Big data challenges and opportunities in the hype of industry 4.0. In: 2017 IEEE international conference on communications (ICC). IEEE
24. Chen M, Mao S, Liu Y (2014) Big data: a survey. Mob Netw Appl 19(2):171–209
25. Jakobik A (2016) Big data security. Comput Commun Netw 12:241–261
26. Cheng C et al (2017) Securing the internet of things in a quantum world. IEEE Commun Mag 55(2):116–120
27. Dubey A, Srivastava S (2016) A major threat to big data: data security. In: Proceedings of the second international conference on information and communication technology for competitive strategies. ACM
28. Tole AA (2013) Big data challenges. Database Syst J 4:31–41
29. Ye H et al (2016) A survey of security and privacy in big data. In: 2016 16th international symposium on communications and information technologies (ISCIT). IEEE
30. Jung JJ (2017) Computational collective intelligence with big data: challenges and opportunities, pp 87–88
31. Gani A et al (2016) A survey on indexing techniques for big data: taxonomy and performance evaluation. Knowl Inf Syst 46(2):241–284
32. Jin X et al (2015) Significance and challenges of big data research. Big Data Res 2(2):59–64
33. Sivarajah U et al (2017) Critical analysis of big data challenges and analytical methods. J Bus Res 70:263–286
34. Bertino E, Ferrari E (2018) Big Data security and privacy. In: A comprehensive guide through the Italian database research over the last 25 years. Springer International Publishing, pp 425–439

35. Chuankun WU (2010) A preliminary investigation on the security architecture of the internet of things. Bull Chin Acad Sci 25(4):411–419
36. Poudel S (2016) Internet of things: underlying technologies, interoperability, and threats to privacy and security. Berkeley Tech LJ 31:997
37. Minerva R, Biru A, Rotondi D (2015) Towards a definition of the internet of things (IoT). IEEE Internet Initiat 14–16
38. Bhabad MA, Bagade ST (2015) Internet of things: architecture, security issues and counter-measures. Int J Comput Appl (0975-8887) 125:1–4
39. Karlo C, Wangner D (2003) Secure routing in wireless sensor networks: attacks and counter measures. Adhoc Netw (Elsevier) 293–315
40. Derbez P, Fouque PA (2014) Exhausting Demirci-Selçuk meet-in-the-middle attacks against reduced-round AES. In: International workshop on fast software encryption, pp 504–558
41. Nyberg K (2015) Links between truncated differential and multidimensional linear properties of block ciphers and underlying attack complexities, pp 162–179
42. Angela McIntyre JE (2013) Gartner, market trends: enter the wearable electronics market with products for the quantified self, July
43. Ponemon Institute LLC (2015) Fifth annual benchmark study on privacy & security of health-care data
44. Symantec: internet security threat report (2015). http://www.symantec.com/security_response/publications/threatreport.jsp
45. Wurm J, Hoang K, Arias O, Sadeghi A-R, Jin Y (2014) Security analysis on consumer and industrial IoT devices. http://jin.ece.ufl.edu/papers/ASPDAC16_IOT.pdf
46. Gachet D, Aparicio F, de Buenaga M, Ascanio JR (2014) Big data and IoT for chronic patients monitoring. In: Hervás R, Lee S, Nugent C, Bravo J (eds) Ubiquitous computing and ambient intelligence. Personalization and user adapted services. LNCS, vol 8867. Springer, Heidelberg, pp 416–423
47. Hernandez G, Arias O, Buentello D, Jin Y (2014) Smart nest thermostat: a smart spy in your home. In: Black Hat USA
48. Teresa Villalba M, de Buenaga M, Gachet D, Aparicio F (2016) Security analysis of an IoT architecture for healthcare. ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. https://doi.org/10.1007/978-3-319-47063-4-48