Chapter 2
A Review of Current Security Issues in Internet of Things

Mudassar Ahmad, Tanveer Younis, Muhammad Asif Habib, Rehan Ashraf, and Syed Hassan Ahmed

Abstract The Internet of Things (IoT) is a framework in which every real-world object can be identified uniquely and has the capacity to send and receive data to the network. This paper presents analysis and survey on IOT security, also discusses the current status and challenges of IOT security. Typically, there are three layers in IoT architecture, i.e. perception layer, network layer, and application layer. For secure internet of things realization, at each layer a number of security principles should be enforced. In the future the implementation of IoT is only possible if the security issues related to each layer are resolved and addressed. A number of researchers try to address and to give corresponding countermeasures to secure each layer of IoT. This paper provides an overview on proposed countermeasures and challenges of Security.

2.1 Introduction

We are living in the age of internet where we are surrounded by many computing devices. Wired and wireless network are now existing in abundance. Future internet will be developed in such a way that every real-world object will be connected and available online everywhere each object will be able to cooperate and interact with each other. As in the future everything will be connected to the internet, we can call the future internet as an Internet of Things (IoT). In the vision of IoT the object of real world will be the part of the internet. It is observed that by 2020 the number of IoT devices will be more than 50 billion [1]. There are many application areas

M. Ahmad · T. Younis · M. A. Habib (✉) · R. Ashraf
Department of Computer Science, National Textile University, Faisalabad, Pakistan
e-mail: mudassar@ntu.edu.pk; tanveeryounis66@gmail.com; drasif@ntu.edu.pk; rehan@ntu.edu.pk

S. H. Ahmed
Department of Computer Science, Georgia Southern University, Statesboro, GA, USA
e-mail: sh.ahmed@ieee.org

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_2

of IoT such as smart home, smart transportation, smart agriculture, smart business, smart grid, smart healthcare, smart cities, smart logistics, and many more. In IoT everything will be interconnected and they must share information with each other. The transmission of information will be take place in the public places i.e. network layer and application layer. So, if there is no effective mechanism for information protection then the information could be stolen which will result in privacy risk, therefore security and privacy are the concerns of IoT enabled devices but it is difficult to implement due to the various diversity of the IoT devices. Therefore, it is very important to figure out the solution for the security of IoT devices.

2.2 Evolution of Internet of Things

Internet connectivity is becoming cheap and easily accessible all over the world [2]. In computing devices, micro and nanotechnology is being introduced which reduced their size and consumption power while enhancing their storage capabilities which makes it easy to equip them with actuators and sensors. This mishmash of small devices with multiple purpose devices enables them to communicate over the internet. RFID tags, NFC tags, or barcode are attached with the physical objects, then devices such as smart phone, tablet, and RFID/NFC readers are used to scan them. The internet capabilities can be enhanced by connecting this combination of bodily world and cyber space through the smart devices. This will result in a new era of internet which is known as Internet of Things. Figure 2.1 [3] gives the picture of future internet.

Fig. 2.1 Generic IoT scenarios

2.3 Generic Architecture of Internet of Things

Different researchers [4, 5] give different opinions about the layers of the IoT. The basic architecture of IoT can be viewed as three layers as shown in Fig. 2.2 [6]. They are named as Perception, Network, and application layers. Security issues are related to each layer. IoT will face a number of challenges in the future especially related to the security and privacy [2]. The main procedure of IoT is to connect everyone with everything to exchange information with each other and the number of communication devices will be increased exponentially. Therefore, improvement in IoT is dependent on the progress of technology and is applicable for the diverse types of application and business models.

2.3.1 Perception Layer

This layer has resemblance to the physical layer in OSI model. The perception layer consists of various types of sensors and actuators (i.e., QR code, RFID, infrared ZigBee, etc.). These sensors collect, sense, and process data (location, vibration, humidity, wind speed, dust in the air, etc.) collected from the environment and transmit this information to the network layer.

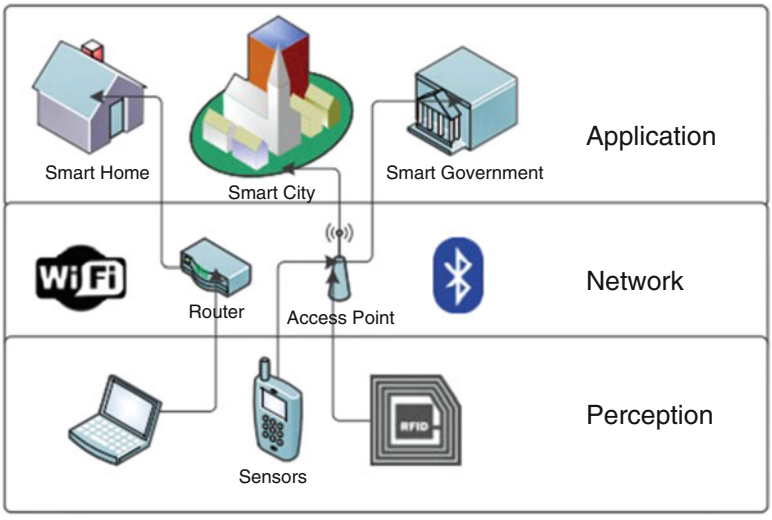

Fig. 2.2 IoT architecture

2.3.2 Network Layer

This layer is responsible for the transmission and routing of the data collected from different IoT sensors to the various IoT devices and hubs over the internet. In this layer, different technologies (i.e., Zigbee, LTE, 3G, WiFi, Bluetooth, etc.) are used to operate various network devices, i.e. router, switches, and gateways. Aggregation filtration and transmission of data take place through network gateways and they serve as a mediator between different IoT devices [7].

2.3.3 Application Layer

This layer is responsible for confidentiality, authenticity, and integrity of the data. The purpose of IoT is achieved at this layer. IoT (internet of things) applications can be smart home, smart postal, smart glasses, smart transportation, smart health, etc.

2.4 IOT Protocols

Protocols are the rules and regulations that are used for end-to-end communication of devices connected to a different or same network. This section will give a brief description about the protocols which are mostly used in machine-to-machine (M2M) communication. Message Queue Telemetry Transport (MQTT) [3] is a client–sever protocol for messaging transportation. It is easy to implement and lightweight. This protocol will run over TCP/IP. Whenever abnormal disconnection occurs MQTT will notify the interested parties about this event through an extraordinary mechanism. Constraint Application Protocol (CoAP) is an application layer protocol that is used for internet devices with resource constrained. This protocol is specially designed for M2M communication such as building automation and smart city. CoAP can be easily translated to HTTP for simplified web integration and it can also provide specialized necessities such as very small overhead, multicast support, and easiness.

2.5 Security Issues

IoT flawlessly joins two distinct worlds into one. There are many limitations and restrictions related to the IoT devices and components, i.e. their computational power and resources and even heterogeneity of devices, which arises new security issues Security challenges of IoT can be divided into two classes: security challenges and technological challenges. Heterogeneity of devices arises

the technological issues whereas security challenges arise due to the principles and functionality that must be followed to establish a secure network. According to the typical architecture of IoT as in Fig. 2.2 some devices or perception sensor is deployed openly where no monitoring system is present [8], which creates vulnerability for outside attackers. Attackers can access these devices and can program them in such a way that these sensors can send data to the register servers as well as to the group of attackers. Secure communication framework for software, processes, things, and people can be developed by following some principles and rules given below.

2.5.1 *Confidentiality*

Data of IoT should be secure and only authorized users should grant access to the data. Users of IoT can be anything it could be, the other network object, human services and machines, or the same network object. IoT sensors should be protected in such a way that they cannot reveal their collected data to other nearby nodes [9]. How the collected data should be managed is also a confidentiality issue that must be tackled. IoT user should be aware of the mechanism of data management that would be applied, and should ensure the protection of the data during the entire process of IoT.

2.5.2 *Heterogeneity*

In IoT there are multiple devices or sensors belonging to different manufacturers and with different abilities based on the complex or simple architecture. The IoT entities also have different versions of their release. They have different technical interfaces and they perform distinct functions, therefore IoT protocols should be designed in such a way that all heterogeneous entities can function together in different situations [10]. The main purpose of IoT is to connect human to device and human to human, in this way it builds a network of heterogeneous things.

2.5.3 *Integrity*

In IoT data is exchanged among many devices and that is why accuracy of data is very important, which means it should be monitored that the data is coming from the right sender and going to the concerned IoT node without any interference either intended or unintended. In IoT communication integrity feature is imposed by maintaining end-to-end security. The endpoints of IoT has very low computational

power, therefore security or cryptography algorithm implementation is difficult on the end nodes of the IoT.

2.5.4 Lightweight Solutions

As the devices of the Iota have very low computational power and lack of memory have lightweight solutions are introduced which have unique security features. These lightweight algorithms execute on IoT devices that have limited capabilities of computation, that's why they should be compatible with devices. In implementation of IoT protocols or authentication of devices, this restriction should be considered.

2.5.5 Authentication

In IoT every entity or node should be able to authenticate other objects and nodes, but this process is not simple as it requires more effort and is quite challenging due to the heterogeneous nature of IoT devices. Sometimes IoT devices have to communicate with other objects for the very first time [11]. Therefore, there is need of a universal authentication mechanism to authenticate the IoT devices in all condition.

2.5.6 Availability

The aim of IoT is to connect everything and to make everything available online. The IoT data should be available to the IoT users at any place and as any time, besides the data of IoT devices should also be accessible or reachable to the IoT users at any time.

2.6 Security Issues in Each Layer of IOT

There are many security threats related to the layers of IoT, each layer is vulnerable to many kinds of security attacks, these attacks can be active or passive and they can be caused by an internal source or external source [12]. Active attack will immediately block the service whereas passive attack can steal information from the IoT network silently without interfering the services. DoS attack can affect at each layer of IoT making the services of the network unavailable. In this section, we will discuss security issues related to each layer of the IoT.

2.6.1 Perception Layer

The most sensitive and attacking layer of IoT is perception layer, the nodes on this layer mostly operate in outdoor environment which makes it most favorite attacking area in IoT network. Wireless technology is used to transmit the signal between the nodes of IoT, therefore its efficiency can be decreased by waves disturbance. Due to the outdoor deployment of the IoT sensors, an attacker can tamper the hardware of the devices. Moreover, the devices on the perception layer consist of sensors, barcode readers, or RFID whose computation capability and power consumption are very low which make them attackable [13]. Spoofing can be used to exploit the confidentiality of this layer which can alternate identity information of IoT devices. Node capture attack can also be made on this layer in which attacker takes over the node and extracts all the information from the node. Nodes can also be replaced by the attacker on this layer.

2.6.2 Network Layer

DoS attacks can be performed easily on the network layer. Passive monitoring and network analyzing is also very common on the network layer [12]. Exchanging data of devices and mechanism of remote access give rise to these types of attacks. If eavesdropper can get the keying material of IoT devices, then secure communication will be conceded. Therefore mechanism of key exchanging should be protected for secure communication of IoT devices. The communication which takes place between the IoT devices is much different from the internet, the reason is that it is not limited to machine to human. Compatibility is the big issue for the security of IoT devices, because of the heterogeneity of the IoT devices currently available protocols cannot be used. Object protection is as important as the protection of the network. Objects should have the ability to defend themselves against any network attack. By developing good protocols this goal can be achieved. The software capabilities should also be increased to make IoT devices strong enough to handle any abnormal situation that can affect their security [14].

2.6.3 Application Layer

There are no global standards and policies for the development of IoT applications, there are many security issues related to the IoT applications. There are many applications and each application has different method of authentication, which makes difficult to ensure the authentication and privacy. The increasing number of connected devices that also share the data will result in an overhead. This overhead will cause an unavailability of the IoT services. During the process of application

development, another issue should also be considered that is who will be the user of the application and how they will interact with the application. There should be some tolls for the users that they can be used to control the data and to decide that what data should be disclosed and who will be the user of data and when they will be using the data.

2.7 Countermeasures for IoT Security

At all three layers of IoT some security measures are required; at physical layer, we need some security measures in data gathering, for transmission and routing on the network layer, and on application layer for maintaining integrity, confidentiality, and authentication [13].

2.7.1 Authentication Measures

In 2011 an authentication scheme was presented by Zhao in [14] for different IoT terminals and nodes. The basic block of the scheme is based on the feature extraction and hashing, for the avoidance of any collision attacks hashing function is combined with feature extraction. There exists irreversibility property in features extraction, this property is also necessary for the insurance of security and it also provides lightweight solution which is required in IoT. This authentication process is implemented when platform wants to transmit the data to any terminal node of IoT. This scheme will also reduce the information that must be sent while improving the security of IoT, but there is no any practical proof in the support of this scheme.

Wen et al. in [11] presented a different method of authentication for sensor node of IoT which is based on ID authentication mechanism. This works on the mechanism of request-reply based on on-time one cipher scheme. The communicating nodes uses a pre-shared matrix to implement this scheme randomly generated coordinate which are generated by nodes are used as a key coordinate. Key itself is not transferred between the parties but the things with that key coordinate are transferred. Then from this coordinate password is generated. This generated password, i.e. key, time stamp, key coordinate and device ID, is used to encrypt all the messages to be sent. Timestamp validation is then used for the communication between the devices, thus on this basis they can also cancel the session. This cipher can also be used in the situation where securing IoT does not involve sensitivity by using same key for different coordinates. For the optimization of security key coordinates can be changed regularly, for a specific structure of IoT. Protecting access controls is also very important for security, it is as important as authentication.

Mahalle addressed these two functionalities in [15]. He presented the idea of Identity Authentication and Capability Access control (IACAC). His research tries

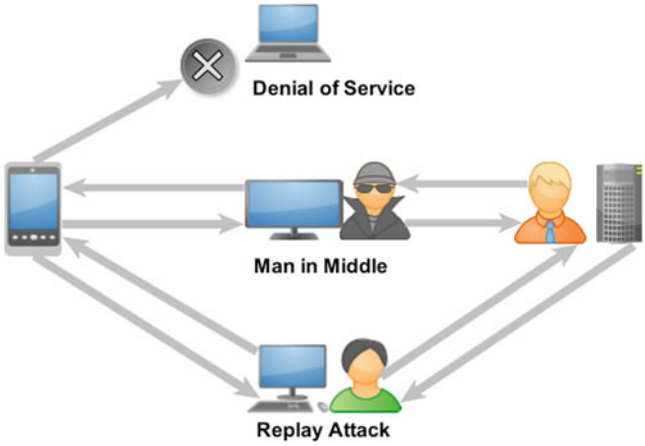

Fig. 2.3 Security attacks modeling of IoT

to achieve the mutual identity establishment in IoT based on both authentication and access control abilities. He proposed a model that uses public key approach which is compatible with distributed, mobile, lightweight, and with the limited computational nature of IoT. Man-in-the-middle attacks are prevented in his technique using a timestamp to authenticate messages between the devices, he called it MAC (Message Authentication Code). Sample use case is shown in Fig. 2.3 [16].

In IOT environment there could be three types of attacks that are Denial of Service, Man in Middle and Reply Attack which is shown in Fig. 2.3.

His scheme is based on three stages; in the first stage, a secrete key is generated, this generated key is based on Elliptical Curve Cryptography-Diffie Hellman algorithm (ECCDH) [16], in the second step identity establishment is taken place by mutual authentication protocols and one-way, at the end implementation of access control is taken place. Public key and private parameter combine to form a shared secret key, and it has low computational overhead due to the use of Elliptic Curve Cryptography (ECC). Using IACAC can minimize significantly because at one time only one ID can have access to the resources.

Perception layer of IoT is mostly based on sensor and RFID. These devices have very limited computational power, therefore on these devices implementation of any cryptography algorithm is very difficult for the network security. For the security of RFID tags, many researchers [17] presented lightweight authentication protocols. If RFID tags are not secured, then attackers can access the network by sniffing (EPC) electronic product key to the target tag and can program it to other tag. By using lightweight authentication protocol these attacks can be prohibited. These protocols ensure the authentication among RFID readers and items that are tagged. Through this mechanism large overhead on these devices is also prevented. A communication scheme is shown in Fig. 2.4 [18] in which RFID tags are to identify the items in IOT environment.

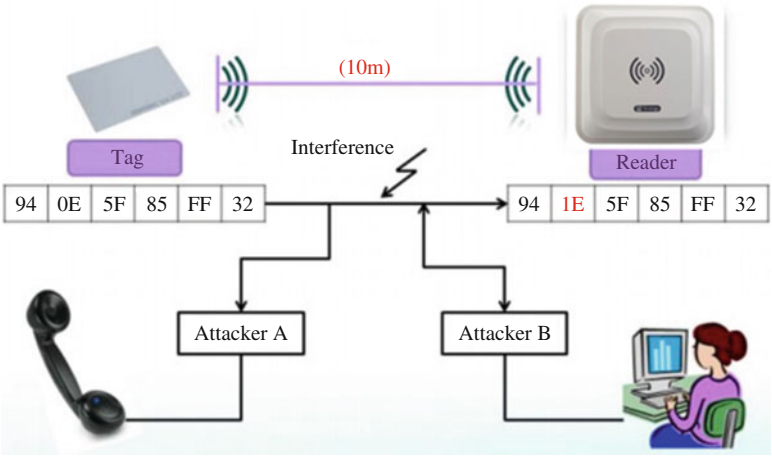

Fig. 2.4 A communication scenario in which RFID tags are used in IoT

2.7.1.1 Digital Certificate

In [19] the authors proposed the method of digital certificate which is attached to the original message to increase the security. A Certificate Authority is responsible for issuing the digital certificate. Certificate Authority verifies the user by giving it a private key. A public key is also announced by the Certificate Authority, it also has its own digital certificate which is known by all the users. This approach is used to eliminate pre-shared key for authentication and introduces digital certificate for the authentication of IOT entities. Figure 2.5 describes the process of issuing the digital certificate to the clients or IOT nodes.

The sequence of operation of the certificate authority is explained with the help of Fig. 2.5 [19].

1. Client requests a source from the server.
2. Server gives its certificate to the client.
3. Certificate contains the digital signature which is signed by Certificate Authority client who also verifies the signature by decrypting it with the CA public key.
4. After verification client also sends his certificate.
5. Digital signature of the client is also verified by the server.
6. After the completion of successful verification server and the client can communicate.

2.7.1.2 Trust Establishment

IoT devices can be moved from one place to the other or the ownership of the devices could be changed, therefore trust establishment is necessary for smooth

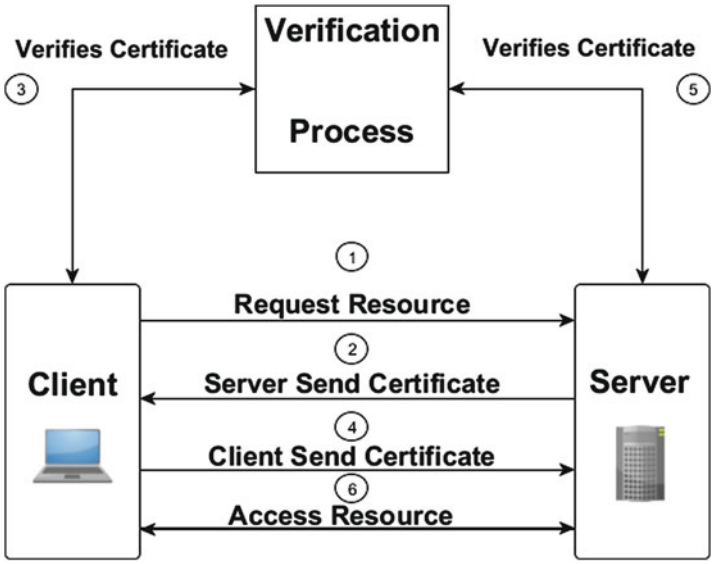

Fig. 2.5 Process of certificate authority

transition w.r.t. permissions and access controls. The concept of mutual interest for inter-system security was presented in [18]. They developed a framework based on the item level access control. In this trust is established in phases from the creation of devices to their operation and transmission. There are two steps in trust establishment; in the first step, the key creation and token. When a device is created, key is assigned to the device. Current owner or the manufacturer can create the token, then these tokens can be used jointly with RFID identification for the Iota devices. Only owner of the device can change these tokens with the condition that the old token is provided. This entire process is much like that, replacing the old key with the new one when new home is bought.

2.7.1.3 Security Awareness

Awareness of the security is very important for the success of IoT framework. Humans which are the part of the IoT network should be aware of security measures. Some researchers in [18] showed the consequences of not securing IoT with actual numbers. They gain access to the various IoT devices, printers, web cameras, etc., these devices were available publicly with no security or they have default access parameters. According to their results many devices were accessible. If in the IoT environment people keep on practicing towards unawareness of the security, by using no security or default security parameters, then the IoT environment will be more harmful than beneficial. If one of the IoT devices is not secured, then hackers can gain access to the whole network through this device.

2.8 Conclusion

Each layer of IoT is susceptible to attacks; therefore, there is need to address security challenges and requirements of IoT framework. For the dynamic mashup of internet of things topology, in the future there is need of new protocols for networking like ipv6 and 5G. Currently, researchers are only focusing on the access control protocols and authentication mechanism of IoT. Currently, the development of IoT is only restricted in small companies and business, for the large-scale development of IoT there is need to overcome many security-related issues of IoT. IoT can transform the way of life we live today. But, in this smart framework security is a big issue. There is high need of new mechanism of identification, software and hardware technology to overcome the security challenges of IoT such as trust management, identification, authentication, privacy, access controls, and confidentiality. If we could address these problems successfully, then soon IoT will transform everything.

References

1. Verizon. (2017). *Intelligent, More Meaningful Business Connections*.
2. Coetzee, L., & Eksteen, J. (2011). The internet of things-promise for the future? An introduction. In *IST-Africa Conference Proceedings, 2011* (pp. 1–9). Piscataway: IEEE.
3. Kraijak, S., & Tuwanut, P. (2015). A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends, 6–6.
4. Zhao, K., & Ge, L. (2013). A survey on the internet of things security. In *2013 9th International Conference on Computational Intelligence and Security (CIS),* (pp. 663–667). Piscataway: IEEE.
5. Mahalle, P. N., Anggorojati, B., Prasad, N. R., & Prasad, R. (2013). Identity authentication and capability based access control (iacac) for the internet of things. *Journal of Cyber Security and Mobility, 1*(4), 309–348.
6. Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015). Internet of things (IoT) security: Current status, challenges and prospective measures. In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 336–341). Piscataway: IEEE.
7. Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future internet: The internet of things architecture, possible applications and key challenges. In *2012 10th International Conference on Frontiers of Information Technology (FIT)* (pp. 257–260). Piscataway: IEEE.
8. Kumar, J. S., & Patel, D. R. (2014). A survey on internet of things: Security and privacy issues. *International Journal of Computer Applications, 90*(11), 20–26.
9. 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), 2266–2279.
10. Farooq, M. U., Waseem, M., Khairi, A., & Mazhar, S. (2015). A critical analysis on the security concerns of internet of things (IoT). *International Journal of Computer Applications, 111*(7), 1–6.
11. Wen, Q., Dong, X., & Zhang, R. (2012). Application of dynamic variable cipher security certificate in internet of things. In *2012 IEEE 2nd International Conference on Cloud Computing and Intelligent Systems (CCIS)* (Vol. 3, pp. 1062–1066). Piscataway: IEEE.
12. Roman, R., Najera, P., & Lopez, J. (2011). Securing the internet of things. *Computer, 44*(9), 51–58.

13. Leo, M., Battisti, F., Carli, M., & Neri, A. (2014). A federated architecture approach for internet of things security. In *Euro Med Telco Conference (EMTC), 2014* (pp. 1–5). Piscataway: IEEE.
14. Zhao, G., Si, X., Wang, J., Long, X., & Hu, T. (2011). A novel mutual authentication scheme for internet of things. In *Proceedings of 2011 International Conference on Modelling, Identification and Control (ICMIC)* (pp. 563–566). Piscataway: IEEE.
15. Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation, 48*(177), 203–209.
16. Lee, J.-Y., Lin, W.-C., & Huang, Y.-H. (2014). A lightweight authentication protocol for internet of things. In *2014 International Symposium on Next-Generation Electronics (ISNE)* (pp. 1–2). Piscataway: IEEE.
17. Xie, Y., & Wang, D. (2014). An item-level access control framework for inter-system security in the internet of things. In *Applied mechanics and materials* (Vol. 548, pp. 1430–1432). Zürich: Trans Tech Publications.
18. Patton, M., Gross, E., Chinn, R., Forbis, S., Walker, L., & Chen, H. (2014). Uninvited connections: A study of vulnerable devices on the internet of things (IoT). In *2014 IEEE Joint Intelligence and Security Informatics Conference (JISIC)* (pp. 232–235). Piscataway: IEEE.
19. Panwar, M., & Kumar, A. (2015). Security for IoT: An effective dtls with public certificates. In *2015 International Conference on Advances in Computer Engineering and Applications (ICACEA)* (pp. 163–166). Piscataway: IEEE.