Indonesian Journal of Electrical Engineering and Computer Science
Vol. 20, No. 3, December 2020, pp. 1685~1692
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v20.i3.pp1685-1692

Internet of things (IoT): a technology review, security issues, threats, and open challenges

Alaa Ahmed Abbood[1], Qahtan Makki Shallal[2], Mohammed A. Fadhel[3]
[1]Faculuty of Business Informatics, University of Information Technology and Communications, Iraq
[2]Management Technical College of Basra, Southern Technical University, Basra, Iraq
[3]College of Computer Science and Information Technology, University of Sumer, Thi Qar, Iraq

Article Info

Article history:

Received Feb 14, 2020
Revised Apr 15, 2020
Accepted May 4, 2020

Keywords:

Application layer
Internet of things
IoT elements
Network layer
Perception layer
Security issues

ABSTRACT

Internet of things (IoT) devices are spread in different areas such as e-tracking, e-commerce, e-home, and e-health, etc. Thus, during the last ten years, the internet of things technology (IoT) has been a research focus. Both privacy and security are the key concerns for the applications of IoT, and still face a huge number of challenges. There are many elements used to run the IoT technology which include hardware and software such as sensors, GPS, cameras, applications, and so forth. In this paper, we have analyzed and explain the technology of IoT along with its elements, security features, security issues, and threats that attached to each layer of IoT to guide the consideration of researchers into solve and understand the most serious problems in IoT environment.

Corresponding Author:

Qahtan Makki Shallal,
Department of Information Technology,
Southern Technical University, Iraq.
Email: qahtan.makii@stu.edu.iq

1. INTRODUCTION

Internet of things (IoT) is proposed in 1999. The concept of IoT can be described as a technology that making objects connected together and having the ability to send and receiving data. Recently, the idea of IoT has grown to be significantly popular by using a range of representative applications, which can include (intelligent transportation, greenhouse monitoring, and telemedicine monitoring) [1-3]. Typically, IoT has many different components which are heterogeneous access, information processing, sensing, services, applications, and various other components which can include privacy and security [4]. In today's scenario, the IoT is almost like a buzzword that is widely known, and many applications are widely increasing in number. The IoT technology may have to face with many challenges because of using IoT will increase the number of devices to the network, in which extends the idea of 'internet' across the sensor network, mobile network, traditional internet, and so forth [5]. Therefore, a new issue of security and privacy will come up includes integrity, authenticity, confidentiality of IoT data [6].

From this point, both the autonomous control and ambient intelligence are not a portion of the IoT original concept. With the improvement of cloud computing, distributed multi-agent control, and advanced techniques of the network, there are endeavors to linking the autonomous control with IoT concept in the research of M2M to generate a transformation of M2M in CPS form [7, 8]. Typically, the CPS focusing on cross-domain optimization, cross-layer optimization, interactive applications, intelligentizing interaction, distributed real-time control, etc. Thus, new technologies must introduce to fulfill the requirements of privacy, security, and reliability.

2. LITERATURE REVIEW

The security and privacy issues that belong to IoT has been discussed in many research papers. Most researchers review the security, as well as privacy, also the available solutions that exist, have been introduced. The work in [9] tries to define the security issues available in every layer of the Internet of Things using specific security measures. However, there is no solution other than encryption the layer of perceptual. The authors of [10], only address IoT security in relation to key security principles, that include integrity, availability, and confidentiality. The authors proposed two-step verification using biometric authentication, which does not apply when communicating from one machine to another. The proposed actions, are not given deep detail and does not discuss the nature of the IoT with similar low-power devices and massive network traffic. The authors in [11] have reviewed many technologies of smart home including sensor technologies, smart home network and appliance, and control systems for smart homes. The home automated prototype has been proposed to make users able to switch on/off any household appliances remotely based on the IoT environment along with solar charger enhancement. There are four types of a prototype of sensors used, which are: temperature sensor, intrusion detection, a sensor for ultrasonic, and smoke gas for control the PIR sensor and automatic environmental. During the work, the test field design, software, and hardware have discussed. As a result, the home appliances have integrated successfully along with the control system of the smart home through relays. The analysis achieved in [12] is addressing the security challenges, threats, and requirements that provide advanced countermeasures for only one security feature to control access. Furthermore, the research work in [13] has accomplished a complete study on the issues of privacy and security in the network of IoT. However, particularly highlights the basic issues of security in IoT as well as security attacks. As a result of this work, twelve various attack types are classified into four level as low, medium, high, and extremely high with their suggested solutions to meeting these attacks. In [14] the authors present and survey main security issues in IoT. The paper has reviewed and classified the most popular issues of security that attached to each architecture layer of IoT, as well as the protocols utilized for management, networking and communication. Further, the security requirements of IoT have outlined the present attacks and threats. In addition, mapping the problems of security in IoT compared to solutions that existed in the literature part of the paper. Finally, discussed the blockchain, and how can be used to solve the security problems of IoT. Further, the authors in [15] have helped the user to discover the empty space in the parking area, which will efficiently reduce the consumption of time and fuel, during the driver is searching the space. The work has Implemented to be work online via the website. In [16], a literature review accomplished to make an integration between Intelligent Transport systems ITS and IoT. The research paper is to discuss the resource privacy, location identification, controller system, and clustering prospect in ITS. By integrating both IoT and ITS, users can increase the optimization of traffic. The authors of [17], has focused on two parts. The first part has explained and categorized the problems of security as well as its solutions for the smart cities. Based on many different factors the security problems and solutions have been categorized, the factors are technological governance, and socioeconomic. This classification delivers an easy observation of existing security solutions, vulnerabilities, and threats for the individual areas of technologies that are introduced during 2010-2015. The second part has tested the architecture smart cities.

3. IoT ELEMENTS

There are three main components required to construct the IoT, these components are hardware components, Middleware components, and Visualization. As shown in Figure 1 the description of IoT key elements.

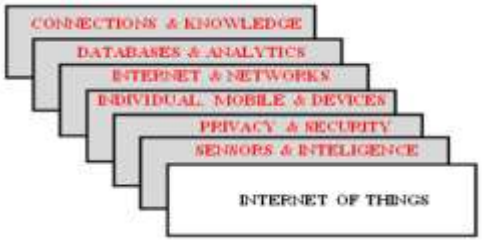

Figure 1. The elements of IoT

3.1. Unique identification for each smart device

IoT consists of a wide range of smart electronic devices. All of these smart devices need a unique identification to obtain communication and helps to access and control remote devices via the internet [2].

Further, Ipv4 is providing a limited range of unique addresses for smart devices. Fortunately, IPv6 supports a large range of unique addresses. In addition to unique address type, each of these smart devices has an object id which typically used to indicate the particular smart device inside the network [18, 19].

3.2. Sensing devices

Each object includes a sensor, which will sense the data continuously depending on the context. The context may be sensing sound level, temperature, or humidity [20].

3.3. Communication

It is the channel used for communication to interchange the sensed data from the smart devices. This media may be Wi-Fi, 3G, 4G, long term evolution-advanced (LTE-A), Radio Frequency Identification (RFID), near field communication (NFC), Z-wave, ultra-wide bandwidth (UWB), or Bluetooth [21].

3.4. Data storage and analytics

In the IoT technology, the smart electronic devices produce a big number of data, these data have to be kept in the specific storage device [22]. Thereafter, this stored data will be analyzed to remove useless information and keep meaningful information. To achieve this, an analytical tool that includes an intelligent algorithm has to be introduced to consider useful information only from raw data. In addition, this analytical tool must support interoperability along with different platforms. In the architecture of IoT, the middleware represents both analytical tools and storage. A centralized infrastructure will be requested to support both analytical tools and storage [23, 24].

3.5. Visualization

Currently, life has turned out to be smart. In fact, by using laptops or smartphones user needs to download the necessary application which will help the user to communicate with the centralized database in order to acquire the useful information relating to the actual environment [25].

4. IoT SECURITY ISSUES AND FEATURES

The main security goals such as (Confidentiality, Integrity, and Availability) are highly required in IoT technology. However, the technology of IoT has many limitations and restrictions in regards to resources of computational and power, devices, and even the IoT's heterogonous as well as ubiquitous nature that presents additional issues. The current section divides into two parts, first: the security features in which the IoT needs to have, and second: the issues of security in each IoT layer [26].

4.1. IoT security features

The IoT security challenges can be classified into two parts; Technological as well as Security [27]. The Table 1 explains the difference between the two parts. There are quite a few facilities to guarantee the basis of security, typically the software that locally installed over all the IoT devices should be highly authorized. The IoT device must authenticate itself to the network as soon as turned on, that has to be done before receiving or sending any data [28]. Due to the limitation of memory capabilities and computation in IoT devices, firewalling is important to filter the network packets that heading for the devices in the IoT environment. The patches and updates on a particular device must be setup using a technique that does not consume additional bandwidth. Beneath are the philosophy of security that should be provided to perform a secure channel for all IoT nodes [29].

Table 1. The difference between technological challenges and security challenges

Technological challenges	Security challenges
It come into sight because of the devices attributes which are heterogeneous and ubiquitous nature.	The security issues belong to the functionalities and principles that must be enforce to accomplish a network security.
It is typically belong to distributed nature, energy, scalability and wireless technologies.	It may require the capability to convey the security with the idea of integrity, end-to-end security, authentication, and confidentiality etc.

4.1.1. Confidentiality

It is really significant to guarantee the data security, and only authorized users are able to access the data. In the technology of IoT, a user may take various shapes such as services, machines, and human, internal devices (which is part of the network), and external devices (which is not part of the network). For instance, it is significant to ensure the sensors are unable to detect the data gathered from the surrounding

nodes [30]. An additional concern of confidentiality is how the network data will probably be controlled. It is essential that the applied management mechanisms must be known to the IoT users, who will be handle the process of management, and to make sure the network data is preserved through the course of action [31, 32].

4.1.2. Integrity

The IoT technology is based upon data interchange among a range of devices. Hence, it is essential to guarantee the data accuracy; which is received from the sender and to make sure that the data received safely without any tampered during the transmission channel [33, 34]. The feature of integrity can be achieved by protecting the end-to-end security of communication in IoT. The management of traveling data is performed by using specific procedures and firewalls, but it unsuccessful to ensure security at the endpoints due to the characteristic nature related to low computational power in the node of IoT.

4.1.3. Availability

Quantity of electronic devices will be joined through the IoT environment. It is essential the IoT users must get the data whenever they required. In addition to that, there are many other components utilized in the technology of IoT; both devices and services will need to available and reachable, whenever they required [2].

4.1.4. Authentication

Each and every IoT device in the same network must have the ability to authenticate and identify other devices. However, this action can be very difficult because of the IoT nature; many entities are required to be implemented (processing units, people, service providers, devices, and services). In addition, there may be one device/devices want to connect with other device/devices for the first time for the purpose of exchange data. Due to the above mentioned, a method must exist to perform the authentication between devices at every interaction inside the IoT [32].

4.1.5. Lightweight solutions

It is undoubtedly a unique feature of security that is revealed due to the restrictions in the IoT device's capabilities such as computational and power. In fact, it is a limitation that needs to be treated during constructing processes of protocols whether they are in authentication or encryption of devices and data in IoT [35]. Because these protocols are supposed to be utilized on the devices of IoT which are limited

4.1.6. Heterogeneity

The IoT connects many different devices with various vendors, accomplishments, and difficulties. In fact, the devices vary, such as functionality, release version and dates, and technology of interfaces. Therefore, the designed protocols must be workable for all devices in the network in any situation. The IoT intends to join one device to another, particular person to device, and person to person, thus IoT provides a way to connect these heterogeneous entities and networks [36]. Moreover, the other issue is the environment which always changing, also a particular device will connect to a group of devices and other time may need to connect to another group of devices. In order to guarantee the security, a system of optimal cryptography is required for suitable security protocols and key management.

4.1.7. Policies

In order to ensure the data are sent, protect, and managed in a productive way, there must be some particular standards and policies. However, the important thing is a mechanism of applying the policies which are required to make certain that any single device is utilizing the standards. Furthermore, service level agreements (SLAs) need to be recognized in all services attached [29]. The existing regulations which used in both computer and network security are probably inappropriate for IoT technology, as a consequence of its dynamic nature and heterogeneous. The execution of these policies will set up a confidence by users in the IoT technology which will contribute to technology growing.

4.1.8. Key management systems

The devices and sensors that belong to the IoT network are required to exchange a number of encryption materials to make sure that the data is confidential [37]. To achieve this, there should be a system of lightweight key management for every framework that could allow confidence among various entities, and distribute keys through a specific process that consuming minimum capabilities of devices.

4.2. Security challenges in IoT layers

Each single IoT layer is vulnerable to attacks and threats. They may be either passive or active type, that might initiate from external/internal forms of the network unsettled to a particular attack from the insider [38].

In fact, active attack straightway breaks the service, whereas the passive type controls the specific details of the IoT network with no need of affecting its service. Further, each individual layer, devices and services of IoT are exposed to Denial of Service attacks (DoS), in which it is able to make the network, resource, or device inaccessible to the authorized users. As shown in Figure 2 are describing a comprehensive analysis of the security concerns attached to each specific layer.

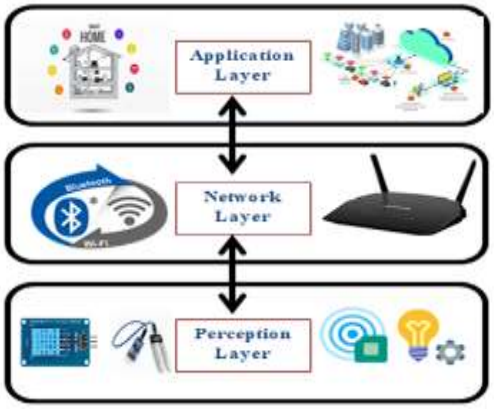

Figure 2. Three layer IoT architecture

4.2.1. Perception layer

Usually, the signals are sent and received among the IoT sensor via the wireless technologies which efficiency can easily compromised using disturbing waves. Therefore, the wireless signals strength must be highly considered [39]. Further, sensor nodes are always used in IoT devices, those devices can be discovered through the network owner as well as attackers also, because those nodes are always operating in outdoor and external environments, causing physical attacks to the devices and sensors of IoT wherein an attacker who can easily tamper the device's hardware components. Also, the character of network topology, that being dynamic as the nodes of IoT are usually moving between dissimilar places. There are many threats that are attached to this layer, such as below [40]:

- Timing attack: This layer's confidentiality can simply be misused by Replay Attack which is prepared through replaying, modifying, or spoofing the data of identity device in IoT [41]. Also, the intruder might acquire the key of encryption through analyzing the time needed to execute the encoding.
- Node capture attack: this type of attack is belong to confidentiality, in which the attacker will take over the device and scan all data.
- DoS attack: The Attacker has the ability to add an additional device to the IoT environment that loom up data integrity in this particular layer through the process of forwarding brute data. Definitely, this could easily result in DoS attack, via the nodes energy-consuming inside the system and prevent the nodes' sleep mode which used to reduce the consumption of energy [42].
- Unauthorized Access to Tags. Because the mechanism of accurate authentication is insufficient with many version of RFID software, the tags can easily used by a certain person devoid of permission. In addition, The attackers are able to do data read, modified, and delete [43].
- Tag Cloning. Because the tags are formed on several objects that observable and also its data are easily modified and read using several techniques of hacking. For that reason, they are often taken using several kind of cybercriminal that's is capable of produce a tag replica and thus compromising it easily in a manner that the reader will not be able to distinguish between the compromised tag as well as the original tag [44].
- Eavesdropping. Due to the specifications of RFID wireless, the attacker will be able to sniff out the information easily, this information is confidential, such as passwords or other data that are flowing from reader-to-tag or tag-to-reader causing it to be exposed as the attacker is capable utilize it in scummy ways.
- Spoofing. It happened when the attacker starts to transmit false stuff of information towards the RFID and pretend as original information [45]. Using this method, the attacker will be able to enter the internal system that makes it at risk.
- Finally, the all above-mentioned security concerns at this layer can be controlled by the help of encryption (that could be end-to-end or point-to-point), authentication (to validate the correct sender identity), and access control.

4.2.2. Network layer

Actually, the adversary is able to attack the privacy and confidentiality at the network layer using traffic passive monitoring, analysis, and eavesdropping. Due to the methods of remote access and data exchange among devices, there is a big chance for these attacks to be executed [46]. The network layer in IoT is extremely vulnerable to the attack of Man-in-the-Middle, that can lead to eavesdropping. In the case of eavesdrop the device's keying material, the secure channel of communication will be completely exposed. The mechanism of key exchange in IoT technology needs to be well secured to protect the data against the process of eavesdropping and then performing identity theft. There is a difference between communication in the internet and communication in IoT as it is not limited to the device to humans. However, the feature of communication between device-to-device contains a Compatibility security issue. The components of network heterogeneity make it tough to use the existing protocols of the network, and still support efficient mechanisms of protection. Attackers can take advantage of everything is connected as a way to obtain additional data with reference to the users, and then utilize this information for the upcoming criminal activities. Therefore, the network protection of IoT is necessary, but in addition, securing the entities belong to the network is evenly necessary. Entities must have the capability to understand the network as well as the facility to secure themselves from any type of network attack. This can be executed by utilizing strong protocols and software that allow entities to react to any circumstances [42, 47]. There are many types of threats that are affected by this layer, as follows:

- Sybil Attack. In this type, the attacker is able to tamper the node to introduce various identities for one particular because the system's considerable part can possibly be disclosed as a result of redundancy's false information [48].
- Sinkhole Attack. In this type the adversary is able to make the disclosed node look like an attractive node to the nodes that are nearby to it; as a consequence of, each and every data flow extracted from any specific node is switched towards the disclosed node which will lead to packets drop; like, silenced of all traffic as the system is cheated to believe that all data are received on another side. Furthermore, this attack will lead to more consumption of energy that may cause a DoS attack [48, 49].
- Sleep Deprivation Attack. The sensor nodes which belong to the network of Wireless Sensor are powered using batteries with not enough lifetime, thus the nodes have used the routines of sleep mode to extend the lifetime of the battery. The type of sleep deprivation will make the nodes awake, this action will lead to fast consumption of battery, which will minimize the battery lifetime in which shutdown the nodes [50].
- Malicious code injection. It is a serious attack, by which attacker will disclose the node and injected the system by malicious code, which will cause the network to be shut down, or even the attacker can do full control on the network [51].

4.2.3. Application layer

There are a lot of security concerns attached to application because at present the IoT does not come with global standards and policies that control the application's interaction as well as development. Each different applications will have different mechanisms of authentication, that will make them tough to guarantee the identity authentication and data privacy. The big number of linked devices in IoT technology that exchange data will definitely cause to applications' overhead which typically analyzes the data, that may have a big influence on the services availability [1, 52]. Also, an issue that needs to be considered at times when constructing a specific applications in the technology of IoT is how several users will communicate with them, the quantity of data that will be revealed, and also who is capable of managing these applications. There are many threats that are attached to this layer, the list of most effective threats are listed below:

4.2.3.1. Threats in application layer

- Malicious code injection: In which the attacker leverage the system attack from the end-user by using some techniques of hacking that permits the attacker to effectively inject any type of malicious code inside the system to take some specific data from the particular user [53].
- Sniffing attack: This is important in this layer, as the system attack will be made using the power of attacker by presenting a sniffer application toward the system, that could obtain information about network causing system corruption [54].
- Denial-of-Service (DoS) Attack. it provides a smokescreen in order to lead the attacks to defensive system breach and hence user's data privacy while cheating the victim by making it believe that the real attack is happening in some other place [55]. This action will put the user's personal details which are non-encrypted under the control of the hacker.
- Spear-Phishing Attack. It is a type of attack that belong to email spoofing, in which the victim is attracted to opening the email that can be used to use the credentials of the particular victim and after that will pretense to gain access for more sensitive information [11, 56, 57].

5. CONCLUSION

The security issues of IoT is a critical part of the technology. This paper described the most popular problems, solutions, and threats in the three layers of IoT. Because IoT technology has required many technologies and devices to be gathered in, many security issues appeared. Therefore, the IoT is still suffering from various issues in security, as it is a new trend in the field of information technology. However, while the environment of IoT has a huge number of devices connected with each other, the security has to be improved to make users reliable to technology during transferring data.

REFERENCES

[1] Atzori, L., Iera, A., & Morabito, G., "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787-2805, 2010.

[2] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M., "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645-1660, 2013.

[3] Kevin Ashton, "That Internet of things thing," 2009. [Online]. Available: http://www.rfidjournal.com/articles/view?4986

[4] Da Xu, L., He, W., & Li, S., "Internet of things in industries: A survey," *IEEE Transactions on industrial informatics*, vol. 10, no. 4, pp. 2233-2243, 2014.

[5] Greengard, S. (2015). "The internet of things," *MIT press*, 2015.

[6] Bokhari, M. U., Shallal, Q. M., & Tamandani, Y. K., "Security and privacy issues in cloud computing," in *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 896-900, 2016.

[7] Restuccia, F., D'Oro, S., & Melodia, T., "Securing the internet of things in the age of machine learning and software-defined networking," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4829-4842, 2018.

[8] Windham, A., & Treado, S., "A review of multi-agent systems concepts and research related to building HVAC control," *Science and Technology for the Built Environment*, vol. 22, no. 1, pp. 50-66, 2016.

[9] K. Zhao and L. Ge, "A survey on the internet of things security," *2013 Ninth International Conference on Computational Intelligence and Security*, Leshan, pp. 663-667, 2013.

[10] M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," *International Journal of Computer Applications*, vol. 111, no. 7, pp. 1-6, 2015.

[11] Gunawan, T. S., Yaldi, I. R. H., Kartiwi, M., Ismail, N., Za'bah, N. F., Mansor, H., & Nordin, A. N., "Prototype design of smart home system using internet of things," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 7, no. 1, pp. 107-115, 2017.

[12] M. Abomhara and G. M. Koien, "Security and privacy in the Internet of Things: Current status and open issues," *2014 International Conference on Privacy and Security in Mobile Systems (PRISMS)*, Aalborg, pp. 1-8, 2014.

[13] Razzaq, M. A., Gill, S. H., Qureshi, M. A., &Ullah, S., "Security issues in the Internet of Things (IoT): a comprehensive study," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 8, no. 6, pp. 383-388, 2017.

[14] Khan, M. A., & Salah, K., "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395-411, 2018.

[15] Dzulkurnain, Z., Mahamad, A. K., Saon, S., Ahmadon, M. A., & Yamaguchi, S., "Internet of things (IoT) based traffic management & routing solution for parking space," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 15, no. 1, pp. 336-345, 2019.

[16] Chand, H. V., & Karthikeyan, J., "Survey on the Role of IoT in Intelligent Transportation System," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 11, no. 3, pp. 936-941, 2018.

[17] Ijaz, S., Shah, M. A., Khan, A., & Ahmed, M., "Smart cities: A survey on security concerns," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 7, no. 2, pp. 612-625, 2016.

[18] Han, D., Anand, A., Dogar, F., Li, B., Lim, H., Machado, M., & Byers, J. W., "XIA: Efficient Support for Evolvable Internetworking," In *Presented as part of the 9th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 12)*, pp. 309-322, 2012.

[19] Madakam, S., & Date, H., "Security mechanisms for connectivity of smart devices in the internet of things," in *Connectivity Frameworks for Smart Devices*, pp. 23-41, 2016.

[20] Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D., "Context aware computing for the internet of things: A survey," *IEEE communications surveys & tutorials*, vol. 16, no. 1, pp. 414-454, 2013.

[21] Tamandani, Y. K., Bokhari, M. U., & Shallal, Q. M., "Two-step fuzzy logic system to achieve energy efficiency and prolonging the lifetime of WSNs," *Wireless Networks*, vol. 23, no. 6, pp. 1889-1899, 2017.

[22] Rathore, M. M., Ahmad, A., Paul, A., & Rho, S., "Urban planning and building smart cities based on the internet of things using big data analytics," *Computer Networks*, vol. 101, pp. 63-80, 2016.

[23] Sparrow, M. K., "The application of network analysis to criminal intelligence: An assessment of the prospects," *Social networks*, vol. 13, no. 3, pp. 251-274, 1991.

[24] Kaufman, L., & Rousseeuw, P. J., "Finding groups in data: an introduction to cluster analysis, *John Wiley & Sons*, 2009.

[25] Bokhari, M. U., Shallal, Q. M., & Tamandani, Y. K., "Cloud computing service models: A comparative study," in *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, pp. 890-895, 2016.

[26] Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S., "Vision and challenges for realising the Internet of Things," *Cluster of European Research Projects on the Internet of Things, European Commision*, vol. 3, no. 3, pp. 34-36, 2010.

[27] Xu, T., Wendt, J. B., & Potkonjak, M., "Security of IoT systems: Design challenges and opportunities," *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, San Jose, CA, pp. 417-423, 2014.
[28] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A., "Security, privacy and trust in Internet of Things: The road ahead," *Computer networks*, vol. 76, pp. 146-164, 2015.
[29] Yaqoob, I., Ahmed, E., Ur Rehman, M. H., Ahmed, A. I. A., Al-garadi, M. A., Imran, M., & Guizani, M., "The rise of ransomware and emerging security challenges in the Internet of Things," *Computer Networks*, vol. 129, pp. 444-458, 2017.
[30] Bokhari, M. U., & Shallal, Q. M., "Evaluation of Hybrid Encryption Technique to Secure Data during Transmission in Cloud Computing," *International Journal of Computer Applications*, vol. 166, no. 4, 2017.
[31] Ropraz, F., "Using RFID for Supply Chain Management," University of Freiburg Schweiz, 2008.
[32] Bokhari, M. U., Shallal, Q. M., & Tamandani, Y. K., "Reducing the Required Time and Power for Data Encryption and Decryption Using K-NN Machine Learning," *IETE Journal of Research*, vol. 65, no. 2, pp. 227-235, 2019.
[33] Gharaibeh, A., Salahuddin, M. A., Hussini, S. J., Khreishah, A., Khalil, I., Guizani, M., & Al-Fuqaha, A., "Smart cities: A survey on data management, security, and enabling technologies," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2456-2501, 2017.
[34] Bokhari, M. U., & Shallal, Q. M., "A review on symmetric key encryption techniques in cryptography," *International Journal of Computer Applications*, vol. 147, no. 10, pp. 43-48, 2016.
[35] Gia, T. N., Jiang, M., Rahmani, A. M., Westerlund, T., Liljeberg, P., & Tenhunen, H., "Fog computing in healthcare internet of things: A case study on ECG feature extraction," on *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, Liverpool, pp. 356-363, 2015.
[36] Reinfurt, L., Breitenbücher, U., Falkenthal, M., Leymann, F., & Riegg, A., "Internet of things patterns for communication and management," in *Springer*, pp. 139-182, 2019.
[37] Thota, C., Sundarasekar, R., Manogaran, G., Varatharajan, R., & Priyan, M. K., "Centralized fog computing security platform for IoT and cloud in healthcare system," *IGI Global*, pp. 365-378, 2018.
[38] Zarpelao, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C., "A survey of intrusion detection in Internet of Things," *Journal of Network and Computer Applications*, vol. 84, pp. 25-37, 2017.
[39] Dardari, D., Closas, P., & Djurić, P. M., "Indoor tracking: Theory, methods, and technologies," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 4, pp. 1263-1278, 2015.
[40] Shancang Li, Kewang Zhang, "Principle and application of wireless sensor network," *M. Beijing: China Machine Press*, 2008.
[41] Cho, J., Yu, J., Oh, S., Ryoo, J., Song, J., & Kim, H., "Wrong siren! A location spoofing attack on indoor positioning systems: The starbucks case study," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 132-137, 2017.
[42] Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I., "Internet of things (IoT) security: Current status, challenges and prospective measures," *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, London, pp. 336-341, 2015.
[43] Feldhofer, M., Dominikus, S., & Wolkerstorfer, J., "Strong authentication for RFID systems using the AES algorithm," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 357-370, 2004.
[44] Thornton, F., & Lanthem, C., "RFID security," *Elsevier*, 2006.
[45] Balduzzi, M., Wilhoit, K., & Pasta, A., "A security evaluation of AIS," *Trend Micro*, pp. 1-9, 2014.
[46] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A survey of ATtacks, Security Mechanisms and Challenges in Wireless Sensor Networks," in *International Journal of Computer Science and Information Security*, vol. 4, no. 1, pp. 1-9, 2009
[47] Roman, R., Zhou, J., & Lopez, J., "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266-2279, 2013.
[48] Karlof, C., & Wagner, D., "Secure routing in wireless sensor networks: Attacks and countermeasures," in *Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, 2003.*, Anchorage, AK, USA, pp. 113-127, 2003.
[49] Baronti, P., Pillai, P., Chook, V. W., Chessa, S., Gotta, A., & Hu, Y. F., "Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and ZigBee standards," *Computer communications*, vol. 30, no. 7, pp. 1655-1695, 2007.
[50] Dina, D., & Downie, K. L., "U.S. Patent No. 9,270,520," *Washington, DC: U.S. Patent and Trademark Office*, 2016.
[51] Wu, B., Chen, J., Wu, J., & Cardei, M., "A survey of attacks and countermeasures in mobile ad hoc networks," *Wireless network security*, pp. 103-135, 2007.
[52] Rittinghouse, J. W., & Ransome, J. F., "Cloud computing: implementation, management, and security," *CRC press*, 2017.
[53] Deogirikar, J., & Vidhate, A., "Security attacks in IoT: A survey," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, pp. 32-37, 2017.
[54] Vashi, S., Ram, J., Modi, J., Verma, S., & Prakash, C., "Internet of Things (IoT): A vision, architectural elements, and security issues," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, pp. 492-496, 2017.
[55] Namuduri, S., "Distributed Denial of Service Attacks (DDoS)-Consequences and Future," *Springer-Verlag New York*, 2006.
[56] Yasin, A., Fatima, R., Liu, L., Yasin, A., & Wang, J., "Contemplating social engineering studies and attack scenarios: A review study," *Security and Privacy*, vol. 2, no. 4, 2019.
[57] Bowen, B. M., Devarajan, R., & Stolfo, S., "Measuring the human factor of cyber security," in *2011 IEEE International Conference on Technologies for Homeland Security (HST)*, Waltham, MA, pp. 230-235, 2011.