Security Challenges and Limitations in IoT Environments

Suha Ibrahim Al-Sharekh[1], **Khalil H. A. Al-Shqeerat**[2]

[1,2] Qassim University, Computer Science Department, Saudi Arabia

Summary
Many regions in the world have recently sought to integrate and apply advanced technologies in various aspects of life. Internet of things applications have become popular in many different areas such as smart homes, e-health, smart cities, and smart connected devices, and many more. However, the rapid proliferation of the Internet of things applications may face many of the security limitations and challenges that have recently become the focus of most researchers in this area. This paper aims to provide a comprehensive overview of security challenges and limitations in IoT environments. Moreover, the survey has been conducted to take the views of researchers and IT experts on the main challenges and limitations of the Internet of things technology.

Keywords:
Internet of Things, Security, Challenges, Limitations, Survey.

1. Introduction

The Internet has great importance in our life. It provides a unique and interconnected system through which devices can connect across the world using a set of communication protocols. In the beginning, the Internet was limited to surfing fixed websites and enabling users to communicate with each other by e-mail service. At present, new and multiple Internet technologies have emerged.

The presence of intelligent devices is significant and become a mandatory part of our daily lives, in which it connects different things remotely at any time. The number of connected smart devices is increasing exponentially day by day, so the Internet of Things (IoT) is the ideal solution for managing and monitoring these smart devices.

The IoT term means connecting various things to the Internet. An intelligent terminal can enable physical components to communicate with each other without the need for human interaction [1].

Kevin Ashton mentioned this idea in 1999 during a presentation at Proctor & Gamble. He used this term to link the idea of radio frequency identification (RFID) to the new Internet theme [2]. At an early stage, the usage of IoT technology is equivalent to the use of RFID technology and connecting it to the Internet.

According to Gartner, 20 billion IoT devices are expected to be connected to the Internet by 2020. In the 1990s, sales points and logistics were the most significant and most promising Internet applications. IoT technology was used to identify goods automatically and share information online. At present, most IoT applications are still just an extension of data collection applications, and not yet intelligent or real dialogue between objects and things [3].

The IoT concept is expressed according to the conceptual framework [4] as shown in Figure 1.

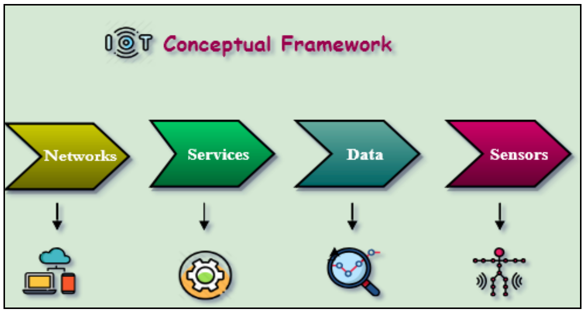

Fig. 1 IoT Conceptual Framework

The development of Internet things plays an essential role in gradually changing human life towards intelligence. Many smart applications rely on IoT technology such as smart home, healthcare monitoring, route planning, building management, and smart city.

IoT is the critical future in the Internet world. Therefore, security services such as privacy and authentication are a crucial factor for modern technologies to achieve the benefits of IoT services [5]. Besides, IoT creates an excellent opportunity for economic growth and life that is more comfortable. However, it causes significant security risks, especially when these devices are compromised or vulnerable to cyber-attack. Therefore, the adoption of adequate security and authentication techniques are necessary for a broad and rapid IoT deployment.

One of the primary motivations behind this study is the spread and growth of IoT usages in various aspects, although many security concerns and issues may arise when adopting IoT different environments. This paper aims to find out the fundamental security requirement, challenges, limitations that affect the adapting of IoT technology.

The rest of this paper is organized as follows. Section II describes the architecture of IoT. Section III overviews the main security requirements of IoT. Section IV reviews some security challenges and limitations that face adopting

Manuscript received February 5, 2019
Manuscript revised February 20, 2019

IoT technology. Finally, the results of the conducted survey are discussed in section V.

2. IoT Architecture

IoT was introduced as a third wave of web pages after static web pages (WWW). A global network connects different types of objects from anywhere, and anytime using Internet protocol (IP) [6].
According to [7, 8], the IoT architecture consists of five layers; perception, network, middleware, application, and business Layers, as shown in Figure 2.

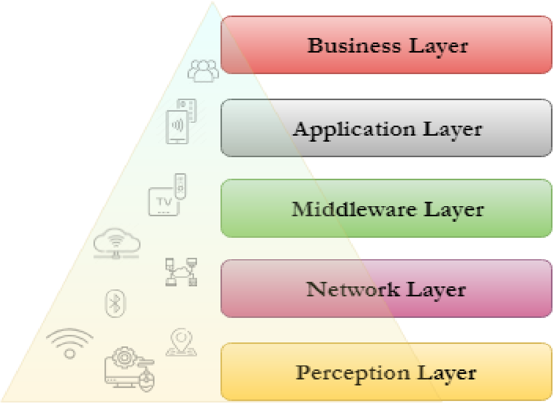

Fig. 2 IoT Architecture Layers

1) Perception Layer
The perception layer is also called the recognition layer. The essential task of this layer is to identify the objects and collect information. This layer consists of a group of physical objects, things. It is responsible for collecting data and providing information to the objects. The responsibility of the layer is to secure how data is collected, stored and transmitted to the network layer. The perception layer includes RFID (Radio-Frequency Identification), sensors, camera, GPS (The Global Positioning System), etc. and it depends on the characteristics of each element, such as protocols or communication technologies used [9].

2) Network layer
The most advanced layer of conventional IoT architecture is the network layer. It likes a neural network and considers the brain of IoT. The network layer is responsible for transferring and processing data provided by the perception layer. It has a significant role in handling the data related to IoT management [10].
The network and communication technology used in this layer such as wired, wireless and satellite depend on the techniques adopted by the perception layer [9]. The perception layer is closely related to the network layer based on communication techniques used such as Wi-Fi, and Bluetooth [11].

3) Middleware Layer
Middleware Layer is also known as a processing layer. It is built over the network layer. In this layer, the IoT systems run [12]. It provides an API (Application Programming Interface) to implement applications. Moreover, it provides many services such as data analysis, data processing, detect and manage devices, data collection, and discovery of information by Object Naming Service (ONS) or Electronic Product Code (EPC). Middleware Layer uses standard protocols that as CoAP, MQTT, XMPP, and HTTP.

4) Application Layer
The application layer contains an application user interface. Applications that are part of the application layer consume web services and application-programming interface that is exposed to the middle layer. It is responsible for delivery and providing various applications in many areas where IoT technology can be deployed and applied, for example, smart homes, smart cities, smart health, and others [13]. The primary goal of the Application layer is to connect IoT users and applications.

5) Business Layer
The business layer manages the whole IoT systems such as applications, business models, and data have been received from the application layer. The business layer develops IoT applications and contributes to the development of successful business models for the promotion of IoT related technologies [14]. Furthermore, this layer should manage and maintain the privacy of users, which is indispensable to the internet of things.

3. Security Requirements

Fundamental security issues in IoT systems require protecting two critical aspects, which are confidential data and identity authentication. Furthermore, five main requirements in information security are considered; data availability, data confidentiality, data integrity, authenticity, and authorization and breach any of these areas will cause security damages or problems to the IoT system [15].
Correspondingly, each of the five layers of IoT must meet these requirements. Figure 3 shows the main security requirements for IoT environment.

a) Data Availability
Data availability is crucial in the IoT. It contributes to ensuring that users have access to the security and reliability of available data. IoT system needs to provide backup of vital information to prevent data loss. Some attacks cause harms related to data availability such as

denial-of-service (DoS) and distributed-denial of services (DDoS) attacks [15].

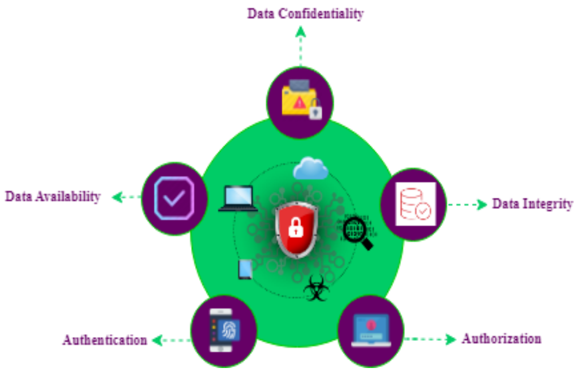

Fig. 3 IoT Security Requirements

b) Data Confidentiality

Data confidentially requires protection of data using specific encryption techniques and mechanisms to prevent data disclosure and any unauthorized access to IoT equipment and devices [16].

c) Data Integrity

Data integrity refers to protecting valuable and sensitive information from the risk cybercriminals. Several things affect data integrity, for example, server downtime. The cyclic redundancy check (CRC) is a way to ensure data integrity and detect message encryption errors by adding a fixed-length value to detect network errors in IoT [15].

d) Authentication and authorization

Authentication and authorization issues play an essential role in IoT security. They verify the identity of users or devices and then grant access to non-suspicious IoT objects or services [17].

4. Security Challenges and Limitations

Although IoT technology offers many advantages and benefits in many areas and solves a range of problems in different sectors, it still faces a range of different security challenges and limitations.

4.1 Security Challenges

Security is the most critical issue that may face IoT development. Providing security for IoT technology is a big and real challenge. Since the IoT technology has a spread scope, and there are many areas of research, we have focused on the security challenges related to some aspects such as performance, work efficiency, costs, data, wireless sensor networks, and other security challenges. In this section, we will explain some of these potential security challenges in the IoT environment.

1. Lack of skills:

Specific skills and expertise are essential factors required for designing, implementing, developing, and managing security that must be considered. The disruption of any of these factors may cause damage to the security system in IoT. Furthermore, lack of skills and expertise cause slow adoption of IoT technologies [18, 19].

The number of skilled people who can adequately handle IoT techniques is very limited. Getting the benefits of IoT technology and dealing with their challenges depends mostly on individual skills.

2. Cost vs. security trade-offs:

The cost plays a crucial role in any project. In IoT, hardware and unit prices are the main contributions to increase security and safety from one side and reduce potential risk on another side. The need for special high-quality equipment requires a high cost of money [20, 21, 22].

3. Privacy protection:

IoT allows anyone to access embedded devices from anywhere, which affects the privacy of sensitive data. Therefore, some norms or rules must be set to avoid the violation of privacy. For example, some of IoT devices sharing the data with other devices and in this case, the data become insecure, which lead in helping the attackers and intruders to penetrate the IoT system, and then insert malicious programs and breach data confidentiality and privacy [23, 24].

4. IoT Architecture challenge:

Internet of things consists of many connected devices and sensors. Each device uses a set of different protocols and standards for communication. There is no well-defined standards and rules for communication [25].

Some researchers have reported that the number of internet-connected devices would exceed 30 billion. Moreover, the applications of IoT would be not limited and would increase day by day. These different devices produced by different manufacturers, even if they do the same functions.

This challenge refers to the nature of IoT and may lead to a lack of unified standardization.

5. Data storage in IoT devices:

As the size amount of data increases at a very high rate, data storage becomes a major problem. Data storage also affects data protection. When stored data damage, it is difficult to back up all stored data [26].

There are no clear criteria to ensure that data distributed within IoT devices is securely transferred to the main data center because the process of transfer data is not synchronized, making it disproportionate to the data center. As we move forward, this is a major challenge for data storage and data management companies in terms of developing tools and standards that address data and provide security correctly.

6. Varying security measures and requirements for IoT components:

Some security measures cannot be implemented because many nodes in IoT lack storage capacity, power, and CPU that make the system very complicated [24].

7. Complicated expanded system:

IoT is a Complex System that can be Widely expanded. Increasing the number of devices, interactions, and people is a reason to increase the risks of data security, and therefore the challenges of managing all these points in the network to maximize security also increase [27, 28].

Another factor to consider is that the necessary components of IoT are wireless sensor networks, which act as data collection by random sensing. Nevertheless, this random density and density of nodes in WSNs lead to difficulty and complexity of the implementation.

8. Limited infrastructure resources:

IoT devices typically have low processing capabilities and limited memory. It is a major challenge for IoT hardware manufacturers and software developers to design comprehensive security measures within a low memory 64KB to 640KB. Moreover, they need to leave enough space for security software to defend against security threats [29]. As a result, the CPU and memory are limited in IoT.

9. Weak security testing and updating:

IoT devices exceed 24 billion Internet-connected devices worldwide. Testing all security-related aspects is difficult. The demand for IoT devices is forcing IoT manufacturers to produce it quickly regardless of the security quality inside them. This challenge makes IoT users vulnerable to security risks and attacks. Some devices may not receive the required security updates. Applying the updates to the IoT devices can be a challenge because some devices do not support updates and some older devices may not support new updates. When the device is not secure, it makes it vulnerable to hacking and other security problems.

10. Lower power sources and capacity:

Power in IoT devices is a crucial factor, in which their battery cannot easily charge, so the capacity is limited and thus failure of the network due to an insufficient battery of the device. Besides, energy efficiency is a significant challenge in the development of IoT devices and their communication protocols. Therefore, energy sources are of great importance, especially in sensor units that have a battery powered.

4.2 Security Limitations

Although the IoT generates many innovations in versatile areas of life and has significant benefits, it contains many limitations that traditional systems are challenging to deal with them. Because the IoT rather complicated system, there are different limitations associated with IoT devices. In this section some security limitations on IoT devices are presented [30, 31, 32]:

4.2.1 Limitations based on the Network

Multi-Protocol Networking: Devices of the IoT may use network protocols (such as non-IP protocol) to communicate between nearby networks. At the same time, it may communicate with an internet service provider via IP. These are multiple features of the communication protocols on the internet of thing, making traditional security schemes inappropriate for devices of IoT.

The diversity of devices: IoT devices are a multiplicity inside the IoT networks, ranging from full personal computer to low radio frequency identification. As a result, it is difficult to find a single security system that can accommodate even the simplest devices.

Dynamic network topology: IoT devices can join or leave the network at any time and anywhere. These temporal and spatial devices make the network topology dynamic. Therefore, the current security of the network does not deal with this sudden type of topological changes, and this model does not comply with the IoT smart devices and does not correspond to its security.

Mobility: One of the most prominent features and characteristics of IoT devices is the mobility feature; that is mean these devices join a close and proximal network without previous configuration. Because of this nature of mobility, we need to develop scalable security algorithms and mechanisms in IoT devices to be compatible with mobility.

4.2.2 Limitations based on the Software

Dynamic security patch: The process of reducing and mitigating the vulnerabilities of the IoT devices', and the process of installing effective security on IoT devices is not a straightforward task. Remote reprogramming may also not be possible for the devices of IoT due to protocols and operating systems, so it may not be able to receive codes and a new library.

Embedded software constraint: Operating systems of IoT that embedded in IoT devices have thin network protocols and may lack module security. Consequently, the security module must be designed for thin protocols.

4.2.3 Limitations based on the Hardware

Tamper resistant packaging: IoT devices may be deployed in many remote areas and left unattended, the attacker may be temper with IoT devices by picking up the devices and can extract encryption secrets, and modify programs or add a malicious contract to them. One of the methods used to resist and defend these attacks is tamper-resistant packaging.

Memory constraint: IoT devices have RAM and flash memory is limited compared to traditional devices such as personal computers and used a lightweight version of General-Purpose Operating System. Therefore, security schemes must be highly efficient for memory. Nevertheless, traditional security algorithms are not designed for memory efficiency because traditional systems use large RAM. Consequently, in IoT devices, security schemes may not have enough memory space due to their small size. Therefore, traditional security schemes cannot be used to secure the devices of the IoT.

4.2.4 Limitations based on WSN

Objects in the IoT are controlled via microcontroller, memory space and often in the power consumption as in wireless sensor networks. At the same time, device protocols, for example, Transmission Control Protocol (TCP) are heavily consumed in the devices. In addition, the IEEE protocol contained in the WSN has a limited maximum transmission unit (MTU) that does not meet the IPv6 primary transmission module. One reason for these limitations makes it possible for developers to use particular protocols for the IoT.

Although wireless sensor networks and ad-hoc networks share similarities, there is a range of limitations that security challenges must overcome. Power management in wireless sensors is a critical problem in wireless sensors network because of low power. Moreover, WSNs do not have the same capacity and memory as in ad-hoc networks. The transmission range also varies between the ad-hoc network and WSNs because the wireless sensor networks are limited in power and therefore have a much shorter communication range than ad-hoc networks. All of these limitations make many security algorithms used in ad-hoc networks, not practical in the wireless sensor networks.

4.2.5 Limitations based on IoT Communication Devices

Devices of the IoT are resources constrained, and therefore, traditional security mechanisms are not precise in smart things. According to [29], there are some security limitations related to the IoT communication devices are:

Memory Capacity: Restricted devices use random access memory (RAM) to store data and storage between a few kilobytes and 12 kilobytes. Data storage in the IoT devices is limited, and some devices cannot store or send data. As a result, some data is ignored if it exceeds the limit of storage.

Energy Capacity: it is the amount of energy the devices have to maintain itself over a specified period. The energy sources in the devices are limited and need to be replaced after a particular time. Some IoT devices consume large amounts of power and are not rechargeable. Therefore. To save the battery in limited devices, use low-bandwidth connections.

Processing Capacity: The processing capacity refers to the amount of power in the devices. Many IoT devices are small, low-cost with low processing capacity. Therefore, these devices require lightweight protocols to work efficiently.

5. Survey and Result Discussion

In this study, we conducted a survey which has been distributed on faculty members, graduate students, IT experts and others who have an interest in IoT.

The survey aims to take their views on the most critical security challenges, and limitations may face IoT. The number of participants that answer to the questionnaire is 190 participants. This questionnaire involves two main research questions as follows:

1- What are the main security challenges face IoT?
2- What is the most limitation currently restrict the spread of IoT?

When reviewing respondents' answers on the questionnaire, found that 11.1% of them did not know IoT security challenges. While 16.3% of participants do not know about the limitations that restrict the spread of IoT. These percentages indicate that people should be more aware of the security issues in IoT since the internet of things is very important and used in many areas, and the orientation will now be on it.

5.1 Main Security Challenges face IoT

The responses to the first question are shown in Figure 4.

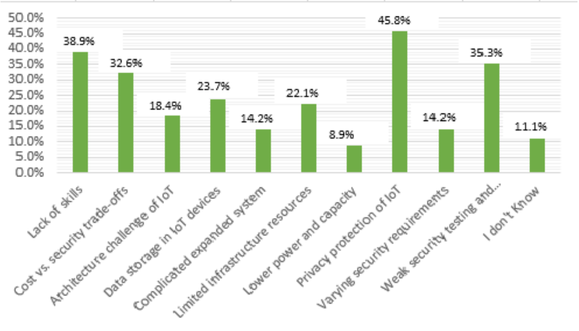

Fig. 4 Security Challenges of IoT

Based on the ratios in the figure. 4 the privacy protection of IoT (with 45.8% votes from respondents), the lack of skills, expertise of IoT adoption (with 38.9% votes from respondents), and weak security testing and updating in IoT devices (with 35.3% votes from respondents) are the most security challenges facing IoT; because these three got the highest vote. Privacy protection is the most significant security challenges because it needs special technologies to protect privacy in IoT. Lack of skills and experience in IoT and weak security testing and updating in IoT devices they have the close voting rate.

Also, some of the security challenges in the questionnaire were observed in ratios such as cost vs. security trade-offs (with 32.6% of respondents), data storage in IoT devices (with 23.7% of respondents), limited infrastructure resources (with 22.1% of respondents), architecture challenge of IoT (with 18.4% of respondents).

Complicated expanded system (with 14.2% of respondents) and varying security requirements and their corresponding measures in IoT environments (with 14.2% of respondents) received the same percentage of voting.

The lowest rating was lower power sources and capacity (with 8.9% of respondents).

5.2 The most Limitations of IoT

Figure 5 represents the opinions of participants on the most limitation currently restrict the spread of IoT.

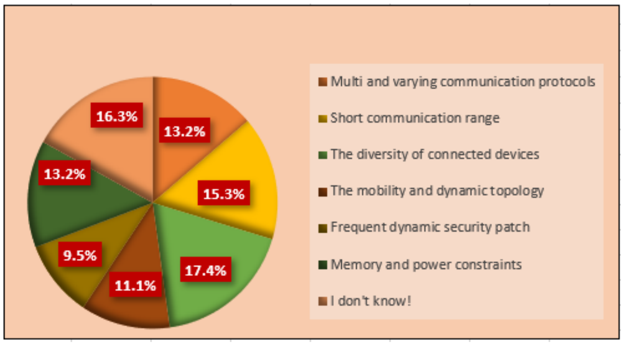

Fig. 5 Limitations of IoT

Limitations are limiting the spread of IoT. From their points of participants' views, the diversity of connected devices got the highest vote rate of 17.4%.

15.3% of participants in the questionnaire have selected a short communication range.

The participants selected memory and power constraints, multi and varying communication protocols, and these two limitations received the same percentage of voting 13.2%.

The mobility and dynamic topology got 11.1% votes. While dynamic security patch got a lower percentage vote of 9.5%.

6. Conclusion and Future Work

This study classified the architectures of IoT based on five layers. We have mentioned the most critical aspects of the security requirements that must be observed in the IoT. Furthermore, the overall security challenges of IoT followed by security limitations related to the IoT devices have been explored. We have conducted a questionnaire on the most critical security challenges and restrictions that face Internet IoT and take people's opinions about it. This questionnaire was distributed to faculty members from various universities in Saudi Arabia, graduate students and IT experts.

This paper provided opportunities for future research work in this area. We believe that this study is important and provides a significant contribution to researchers in developing IoT security. Several potential security issues must be followed for future research, such as vulnerabilities, threats, and provide practical solutions to overcome IoT security threats.

References

[1] Vermesan, O. and Friess, P. eds., 2014. Internet of things-from research and innovation to market deployment (Vol. 29). Aalborg: River publishers. Ashton, K. (2009). That 'Internet of Things' thing. RFID Journal, 22, 97–114.

[2] Minerva, R., Biru, A. and Rotondi, D., 2015. Towards a definition of the Internet of Things (IoT). IEEE Internet Initiative, 1, pp.1-86.

[3] Evdokimov, S., Fabian, B., Günther, O., Ivantysynova, L. and Ziekow, H., 2011. RFID and the internet of things: Technology, applications, and security challenges. Foundations and Trends® in Technology, Information and Operations Management, 4(2), pp.105-185.

[4] Chase, J., 2013. The evolution of the internet of things. Texas Instruments, p.1.

[5] Atzori, L., Iera, A. and Morabito, G., 2017. Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm. Ad Hoc Networks, 56, pp.122-140.

[6] Silva, B.N., Khan, M. and Han, K., 2018. Internet of things: A comprehensive review of enabling technologies, architecture, and challenges. IETE Technical Review, 35(2), pp.205-220.

[7] Atzori, L., Iera, A. and Morabito, G., 2010. The internet of things: A survey. Computer networks, 54(15), pp.2787-2805.

[8] Khan, R., Khan, S.U., Zaheer, R. and Khan, S., 2012, December. Future internet: the internet of things architecture, possible applications and key challenges. In Frontiers of Information Technology (FIT), 2012 10th International Conference on (pp. 257-260). IEEE.

[9] Bilal, M., 2017. A Review of Internet of Things Architecture, Technologies and Analysis Smartphone-based Attacks Against 3D printers. arXiv preprint arXiv:1708.04560.

[10] Gaitan, N.C., Gaitan, V.G. and Ungurean, I., 2015. A Survey on the Internet of Things Software Architecture. International Journal of Advanced Computer Science, 6, pp.140-143.

[11] Zachariah, T., Klugman, N., Campbell, B., Adkins, J., Jackson, N. and Dutta, P., 2015, February. The internet of things has a gateway problem. In Proceedings of the 16th international workshop on mobile computing systems and applications (pp. 27-32). ACM.

[12] Burhan, M., Rehman, R., Khan, B. and Kim, B.S., 2018. IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. Sensors, 18(9), p.2796.

[13] Sethi, P. and Sarangi, S.R., 2017. Internet of things: architectures, protocols, and applications. Journal of Electrical and Computer Engineering, 2017.

[14] Wu, M., Lu, T.J., Ling, F.Y., Sun, J. and Du, H.Y., 2010, August. Research on the architecture of Internet of Things. In Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on (Vol. 5, pp. V5-484). IEEE.

[15] Suo, H., Wan, J., Zou, C. and Liu, J., 2012, March. Security in the internet of things: a review. In Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on (Vol. 3, pp. 648-651). IEEE.

[16] Miorandi, D., Sicari, S., De Pellegrini, F. and Chlamtac, I., 2012. Internet of things: Vision, applications and research challenges. Ad hoc networks, 10(7), pp.1497-1516.

[17] Salman, O., Abdallah, S., Elhajj, I.H., Chehab, A. and Kayssi, A., 2016, June. Identity-based authentication scheme for the internet of things. In IEEE Symposium on Computers and Communication (ISCC), pp. 1109-1111.

[18] Mainetti, L., Manco, L., Patrono, L., Sergi, I. and Vergallo, R., 2015, December. Web of topics: An iot-aware model-driven designing approach. In IEEE 2nd World Forum on Internet of Things (WF-IoT), pp. 46-51.

[19] Lee, I. and Lee, K., 2015. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons, 58(4), pp.431-440.

[20] Kumara, N.M. and Mallickb, P.K., 2018. Blockchain technology for security issues and challenges in IoT. Procedia Computer Science, 132, pp.1815-1823.

[21] Alharby, S., Harris, N., Weddell, A. and Reeve, J., 2018. The security trade-offs in resource constrained nodes for iot application. International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, 12(1), pp.52-59.

[22] Aman, W. and Snekkenes, E., 2015, December. Managing Security trade-offs in the internet of things using adaptive security. In 10th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 362-368.

[23] Middha, K. and Verma, A., 2018. Internet of Things (Iot) Architecture, Challenges, Applications: A Review. International Journal of Advanced Research in Computer Science, 9(1).

[24] Haroon, A., Shah, M.A., Asim, Y., Naeem, W., Kamran, M. and Javaid, Q., 2016. Constraints in the IoT: the world in 2020 and beyond. Constraints, 7(11).

[25] Burhanuddin, M.A., Mohammed, A.A.J., Ismail, R. and Basiron, H., 2017. Internet of Things Architecture: Current Challenges and Future Direction of Research. International Journal of Applied Engineering Research, 12(21), pp.11055-11061.

[26] Alansari, Z., Anuar, N.B., Kamsin, A., Soomro, S., Belgaum, M.R., Miraz, M.H. and Alshaer, J., 2018, August. Challenges of Internet of Things and Big Data Integration. In International Conference for Emerging Technologies in Computing, pp. 47-55.

[27] Gaur, A., Scotney, B., Parr, G. and McClean, S., 2015. Smart city architecture and its applications based on IoT. Procedia computer science, 52, pp.1089-1094.

[28] Hernandez-Bravo, A. and Carretero, J., 2014. Approach to manage Complexity in Internet of Things. Procedia Computer Science, 36, pp.210-217.

[29] Bello, O., Zeadally, S. and Badra, M., 2017. Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT). Ad Hoc Networks, 57, pp.52-62.

[30] Hossain, M.M., Fotouhi, M. and Hasan, R., 2015, June. Towards an analysis of security issues, challenges, and open problems in the internet of things. In 2015 IEEE World Congress on Services (SERVICES), pp. 21-28.

[31] Bellavista, P., Cardone, G., Corradi, A. and Foschini, L., 2013. Convergence of MANET and WSN in IoT urban scenarios. IEEE Sensors Journal, 13(10), pp.3558-3567.

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