Applied Computing Journal https://doi.org/10.52098/acj.202136
ISSN: 2788-9688 Volume 1, Issue 2, pp 103-118, April 2021
Received: 31/5/2021 Revised: 5/6/2021 Accepted: 5/6/2021

Internet of Things: Layers, possible attacks, secure communications, challenges

Ameera A. Al-blushi[1,*] and Mohammed J. Yousif [2]
[1]Department of Computing and Information Technology, Sohar University, Oman
[2] Department of Computer Science, Faculty of Science, Memorial University, Canada
* Corresponding author: Ameera A. Al-blushi[1], meraaalblushi@gmail.com.

Abstract

With the increasing need for information transmission globally for commerce, education, medicine, and other fields, the need for a safe and easy way to use software and hardware efficiently has arisen. The concept of contracting the Internet of Things (IoT) is to enhance the quality of connecting and exchanging data with others, improve implementation of works, increase productivity, and deliver all services efficiently and ubiquitously. The core idea of this technology is to embed different types of sensors along with devices to gather information and perform an action based on analysis of that information. This paper aims to review and explore the main concept of IoT, how it works, layers of intelligence system, possible attacks in each layer, and significant challenges associated with IoT and its potential solution. In addition, it will analyze the studies based on evaluation factors.

Keywords*:* IoT; M2M; smart devices; IoT Cloud Platform; ICT; IoT Protocol; information system

1. Introduction

IoT technology allows users, systems, and devices to connect to large-scale networks, which will expand physical and digital connectivity. Adopting IoT technology is increasing the digital transformation that is a priority for many organizations and governments (Farahani et al., 2021). The latest recorded report of "Statista" indicates that the industrial Internet of Things markets globally is growing twice from 2017 to 2025 (Statista, 2021). The market size of the industrial Internet of Things in 2020 is determined to 77.3 billion U.S. dollars, and in 2025 is expected to be 110.6 billion U.S. dollars, as shown in Figure 1.

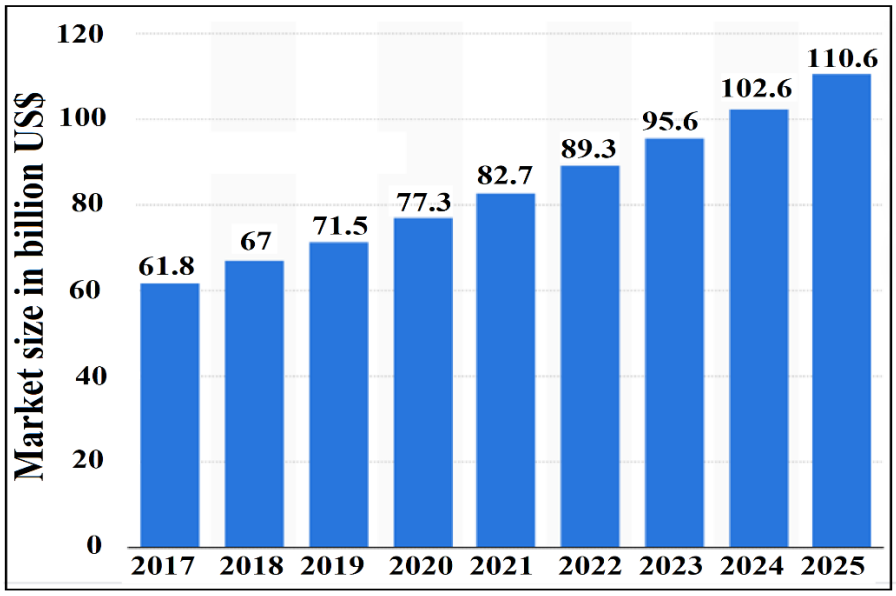

Figure 1. the industrial IoT market size worldwide from 2017 to 2025* (The expected rate) (billion U.S. dollars) (Statista, 2021).

IoT is an effective technology for designing an automated system that collects information from devices via sensors, analyzes it, and then responds with intended actions to meet individual demands, as shown in Figure 2 (AlKishri & Al-Bahri, 2021; FNH & Azeez, 2021). Hence, it is defined as the network of physical things or objects embedded with various technologies, including software, sensors, smart devices for connecting, exchanging information with other computing devices, and systems easily over the network (Marwedel, 2021).

The IoT implementation is growing dramatically (IoT-analytics, (2021):

- In 2018, adapted 8 billion IoT devices.
- In 2019, the IoT devices spread to 10 billion
- In 2020, expected to reach 11.7 billion IoT devices.
- By 2021, it is expected to deploy 13.8 billion IoT devices globally.
- By 2025, it is estimated that more than 30.9 billion IoT devices will connect globally.

On the other hands, Cloud Platform allows the IoT users easily customized software and hardware services that empower IoT functionality and applications. The IoT Cloud Platform access is a subscribed service through specific companies. The IoT provider creates cloud platforms based on the needs of the company specification (Al-Shezawi et al, 2017; Yousif & Alattar, 2017). It allows them to analyze and process the data sent by IoT-enabled devices housed in the cloud storage of the IoT provider (Saini et al, 2011; AL-Balushi et al, 2017; Raut et al, 2011).

Deployment of IoT in these few years has been reduced due to the high cost of implementing it, some potential challenges, and security gaps. Therefore, this research paper attempts to provide effective solutions to protect each IOT, overcome IoT vulnerabilities, and improve security and privacy. This research paper will involve the following sections: Section 2 will briefly explain the work procedure of IoT. Section 3 will discuss the main layers of IoT: perception layer, network layer, and application layer. Section 4 will clarify some potential attacks on each layer and effective solutions to increase the level of security at that level. Section 5 will state how to maintain a secure communications framework. Section 6 will cover some challenges behind the construction of this technology. Section 7 will illustrate the main reasons for adopting IoT in the business environment.

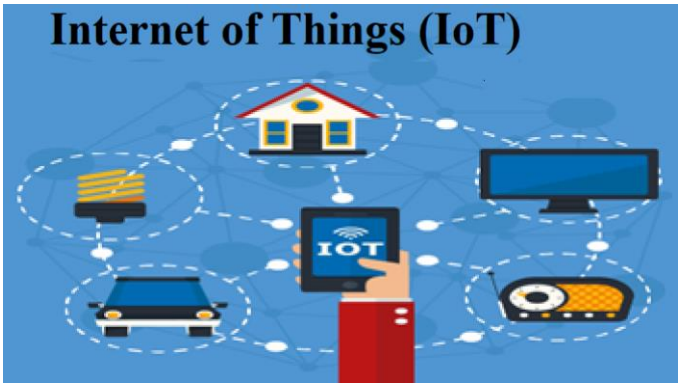

Figure 2. IoT architecture

2. Discussion

Online administration of SETs in this study was associated with lower response rates, yet it is curious that online courses experienced a 10% increase in response rate when all courses were evaluated with online forms in Year 3. Online courses had suffered from chronically low response rates in previous years, when face-to-face classes continued to use paper-based forms.

3. The IOT works

Online administration of SETs in this study was associated with lower response rates, yet it is curious that online courses experienced a 10% increase in response rate when all courses were evaluated with online forms in Year 3. Online courses had suffered from chronically low response rates in previous years, when face-to-face classes continued to use paper-based forms.

Figure 3 illustrates the fundamental work procedure of an IoT system that includes three main phases, which are: initially gather information, then transfer data, finally analyze collected data, and respond with specific actions (Nardelli et al., 2017). Various technologies and tools critically are involved in completing of these phases, such as sensors, gateway, router, and cloud.

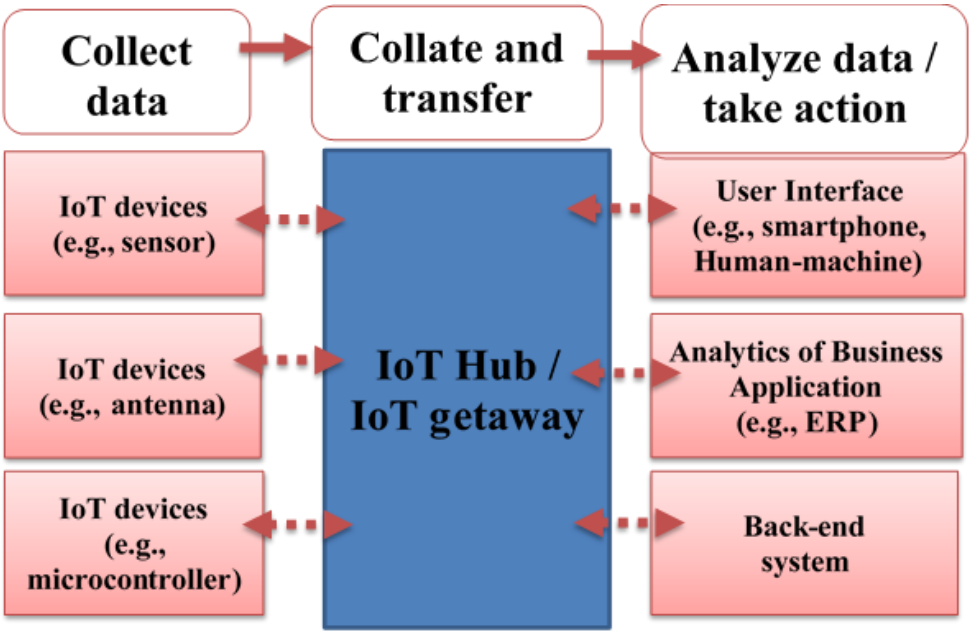

Figure 3. IOT system work procedure

Typically, IoT systems compose several web-enabled smart devices embedded with particular kinds of sensors or communication hardware tools to aggregate and exchange information gained from the deployment environment over the network. For instance, reading temperatures from the observed environment, then acting based on data to perform intended tasks. Usually, IoT devices will establish connectivity with other computing devices, clouds, or systems through the utilization of an IoT gateway or IoT hub to share and transfer data. The information will be transferred to the cloud to be analyzed, or either it can explore locally. Once data is received in the cloud, and after processing it, check if the temperature is acceptable. Also, check if the software will implement required actions to respond to the analysis stage as sending notification alerts to the user or automatically adjacent to the devices if human intervention

is not needed. However, if the user's input is required, the user interface will allow them to enter required data and then transfer it back from the system to the cloud to perform desired changes (Fortino et al., 2014).

4. IoT Layers

The generation of any intelligence system involves three main layers: the perception layer, network layer, and application layer, as presented in Table 1. These layers are required to form the overall architecture of IoT. Each layer integrates various technologies to achieve it is roles.

Table 1. summary of IOT layers

Ref	Layer	Use	Purpose
(Mahmoud et al., 2015). (Atzori et al., 2012).	Perception Layer (Sensing layer)	Sensors	1. This layer uses sensors, and actuators to gatherdata from environment. 2. This layer firstly identifies, gather, process data,then transfer it to network layer.
(Mahmoud et al., 2015). (Atzori et al., 2012).	Network Layer (transmission layer)	Gateway, Router	1. This layer uses router, and gateway to transmitdata for different IOT devices over internet. 2. The gateway of network form as intermediaryamong IOT devices to collect, filter, transmit data to, and from sensors. 3. Router, switch, gateway devices function via various technologies such as WiFi, LTE,Bluetooth, 3G, Zigbee, etc.
(Mahmoud et al., 2015). (Atzori et al., 2012).	Application Layer (management layer)	Cloud, Computing, Servers, DB	1. This layer is used to ensure that data is not modified (integrity), data visible only to authorized parties (confidentiality), and ensure authenticity. 2. This layer provides efficient processing, and analysis of data to response with some actions. 3. At this layer the smart environment will becreated.

5. Discussion Possible attacks at each layer

Online Several security challenges may face each layer of IoT architecture while carrying its responsibilities. Each layer is vulnerable to various attacks, such as conducting a DOS attack (denial of service arrack). And diverse security threats that generally appear due to lack of management, monitoring, or even existence of security gaps lead to increased opportunities for attacks where sometimes IoT devices, networks, resources, and services will be unavailable to authorized individuals when requested (Roman et al., 2013). Ref 10 (Abomhara & Køien, 2014).

The attacks at each layer as follows:

5.1. Perception Layer:

In this layer, attackers can compromise both confidentiality and integrity of data while transmitting it between IoT nodes or even cause physical damage to utilities. This layer is susceptible to several attacks such as:

- Reply attack: Attackers will spoof the address of devices, change, or even replay accurate identity information of any IoT devices, and then pretended as if it is an actual node (Roman et al., 2013).
- Timing attack: Attackers will have the ability to intercept or catch key encryption through analysis of the time required for performing encryption (Roman et al., 2013).
- Node Capture attack: Attackers can eavesdrop on data transmitted between IoT devices by inserting fake nodes (Abomhara & Køien, 2014).
- Malicious Data: Attackers can insert fake nodes in the network to compromise data integrity through transmitting malicious data (Abomhara & Køien, 2014).

Solution for protecting perception layer:

The previous security issues can be addressed through implementation of encryption, authentication (to prove exact identity of source), access control (physical and technical), security measures, secure protocols (Roman et al., 2013; Abomhara & Køien, 2014).

5.2. Network Layer

IoT devices utilize Machine to Machine communication to contact each other's, but users usually will not have direct control over what devices or systems are involved in the communication procedure. Since these devices are connected over the network, this will potentially raise serious threats that attackers can exploit. This layer has more likelihood for the occurrence of attacks:

- DOS attack: Attacker will control services' availability by creating huge overhead over applications. As a result, they disable authorized parties from accessing resources and breach confidentiality (Abomhara & Køien, 2014).
- Man in the middle attack: attackers will compromise communication channels through eavesdropping of the network, traffic analysis, and passive monitoring. And catch key of devices (Abomhara & Køien, 2014).

Solution for protecting network layer:

It is essential to offer protection measures to IoT devices and secure the overall network against attacks. This could implement through implementing encryption, secure protocol, firewall, IDS, IPS, secure protocol, secure channel, and good software that enable objects to respond to any abnormal behaviors (Roman et al., 2013).

5.3. Application Layer

Attackers can potentially target IoT systems and control availabilities of services, resources, and data disclosure through creating massive requests over the applications that analyze data. They can conduct DOS attacks, Malware injection attacks, and other attacks. Therefore, security challenges at this layer are:

- Different authentication: Integration of all IoT applications became a challenging process because each involved application will prerequisite distinct authentication approaches to ensure data privacy, authenticity, and identity (Roman et al., 2013).
- Availability of services: There are a massive amount of connected devices that share data among themselves. In turn, this causes serious overhead over e applications that investigate data. As a result, services become inaccessible (Abomhara & Køien, 2014).

When designing an IoT application, should consider the following concepts:

I. The way clients will interact with them.
II. The size of data that will expose, and to whom.
III. The party that will responsible for managing these applications.

Solution for protecting application layer

The security measures can increase by protecting management parties like a cloud system, communication medium, use of DB logs, IDS, IPS, authentication, and efficient key management (Abomhara & Køien, 2014; Roman et al., 2013).

6. Discussion Secure communications

Security challenges in IoT technology can be classified into two different categories which are: technological challenges and security challenges. Technical challenges will arise due to the heterogeneous issues and distributed nature of IoT devices, such as integrating various technologies as various sensors with distinct capabilities in the environment (Roman et al., 2011). However, security challenges referred to the procedure of achieving secure communication through the integration of the following concept: authentication, end-to-end security, and confidentiality, etc. (Roman et al., 2011). Several security principles must apply to gain a secure communication framework in an IoT environment:

6.1. Confidentiality

It is critical to ensure that data is only visible to authorized individuals, devices, or objects by preventing unauthorized access. For example, it is imperative to ensure that sensors embedded on devices will never expose gathered data for unauthorized neighboring devices. The core issue in the confidentiality feature is how to manage data. Hence, IoT users should be aware of data management approaches that will follow, responsible for performing management, and ensure that they will secure data throughout the whole process (Roman et al., 2011).

6.2. Integrity

During transmission of data among IoT devices, it is critical to ensure that data has not been tampered with by unauthorized individuals and ensure that data came from the right source. The integrity feature can be achieved by maintaining end-to-end security throughout IOT communication which in turn assists in preventing unauthorized modification of data. Also, it can manage data traffic through the utilization of security protocol and the use of a firewall (Roman et al., 2011; Leo et al., 2014).

6.3. Availability

IoT environment connects numerous amounts of devices to deliver intended demands for users. It is critical to ensure that the required data is always available to authorized individuals when needed. As well, not only should data be accessible, but also the involved devices and services should be available when requested via users on time to achieve IoT goals (Roman et al., 2011).

6.4. Authentication

All nodes involved in the IoT environment should have the ability to authenticate and identify all other nodes in the communication process. But this procedure is a challenge since there are numerous entities involved in the procedure, such as various devices, many individuals require services, providers of service, and processing units. Another critical challenge is sometimes; the device may need to interact with an unknown device for the first time. Thus, they should mutually authenticate entities of IoT for every interaction (Leo et al., 2014).

6.5. Lightweight solution

Lightweight feature is a robust security solution generated due to restrictions in power and computation capabilities of devices participating in IoT. These restrictions should be considered while designing or applying protocols in encryption data or the authentication process. However, they should use lightweight algorithms on IoT devices that have limited capabilities. These algorithms can be compatible with IoT devices' limited capabilities while running on it, hence solving this issue (Roman et al., 2011).

6.6. Heterogeneity

IoT environments provide connections among different heterogeneous things that have distinct abilities, limitations, complexities, versions, configurations, and even interfaces, but they should still be cooperative. For instance, secure protocols should be designed to operate in various devices and various situations (Leo et al., 2014). Another critical challenge that must consider is the dynamic environment in which the device, at one time, may connect device to a diverse set of devices. Therefore, to ensure secure communication among devices, an optimal cryptograph system should be maintained with the proper key management (Roman et al., 2011).

6.7. Policies

Various policies and standards must be involved in the IoT environment to guarantee that data will be gathered, protected, managed, and transferred efficiently. Hence, implementing a particular mechanism to ensure that all involved entities follow the defined standards in the required step (Leo et al., 2014). For example, SLA (service level

agreement) should be stated for every provided service. But some current policies related to computer and network security are not valid with IoT because of its heterogeneous environment. Imposing such policies will result in notable growth and wide scalability (Roman et al., 2011).

6.8. Key management

Data encryption will help ensure high confidentiality and high data integrity while transmitting it among IoT devices. Data should be transferred or stored in encrypted form by utilizing suitable cryptography mechanisms. Therefore, efficient and optimal key management should be deployed in the IoT environment for all frameworks, which will establish great trust among all devices. At the same time, maintain secure key distribution, and prevent interception of critical data (Roman et al., 2011).

Online administration of SETs in this study was associated with lower response rates, yet it is curious that online courses experienced a 10% increase in response rate when all courses were evaluated with online forms in Year 3. Online courses had suffered from chronically low response rates in previous years, when face-to-face classes continued to use paper-based forms.

7. IOT challenges

Online administration of SETs in this study was associated with lower response rates, yet it is curious that online courses experienced a 10% increase in response rate when all courses were evaluated with online forms in Year 3. Online courses had suffered from chronically low response rates in previous years, when face-to-face classes continued to use paper-based forms.

Typically, IoT devices utilize Machine to Machine communication(M-M), in which users may not have directed control over what devices or systems IoT devices will communicate with. Therefore, the connection of various IoT devices over network will potentially raise significant threats and challenges that attacker can exploit in an unauthorized manner. Recently, several types of research attempt to address serious issues and challenges associated with the construction of IoT system along with their potential solutions, as depicted in Table 2:

In Leal & Atzori. 2010), the authors describe how to establish secure connection between several devices, and networks in an IoT environment through utilization of MANET technique which also known as Mobile Adhoc Network. MANET is secure type of wireless network connection that able to change its location, and configure itself

quickly. It uses a wireless connection to connect distinct things. In (Misra et al., 2010), the researchers present how to ensure successful, and secure delivery of data (packets) even in the presence of failures between nodes of IoT through utilizing the concept of cross-layered and Learning automates (LA) based on fault-tolerant routing protocol. This protocol is designed to be highly adaptive, and scalable in order to over better performance in heterogeneous environment, and case of fault.

In (García et al., 2014), the authors argue how to recover from heterogeneous challenges by utilizing graphic editor technology that produces a model defined via a Domain Specific Language (DSL). DSL gives an excellent opportunity to improve interactions, and collaborations between heterogeneous devices in the IoT environment. Also, it is used to enhance the programmability or simplify the procedure of diverse wiring components of an IoT system. In (Ali et al., 2015), the authors apply adaptive Semantic Interoperability Architecture (SIA) to produces adaptive architecture that facilitates the accessing of information and to ensure that IoT devices from different vendors are effectively interoperable with each other's in the heterogeneous environment, as a result, improve performance.

In (Ming et al., 2013), the researchers cover QOS (Quality of Service) feature in IoT environment to ensure the quality and performance of services delivered to meet expectations and satisfy IOT main goals. They presented a comparison between three algorithms to identify QOS metrics for IoT services. The result shows that the BT algorithm (Burst Tolerance) is more suitable for IoT environments than IP and GA (Genetic Algorithm) algorithms since it can offer highly scalable services and real-time applications. In (Gubbi et al., 2013), the authors investigate the scalability, and availability issues in the IoT environment. They provide a general overview of practical approaches to construct scalable architectures that handle large bound of requests, provide efficient data processing and management through utilization of cloud computing (private, public, and hybrid cloud).

In (Alam et al., 2010), they implement IOT Virtualization Framework (VF) based on SenaaS (Sensor-as-a-Service) technology to increase functionalities of embedded sensors. Then, this, in turn, will enhance the performance of IoT devices and their work pattern. The virtualization technique provides a flexible and adaptive interface to facilitate manipulation and interaction with IoT nodes. In (Liu et al., 2015), the authors display a critical challenge: big data processing and management. They discuss handling and processing a massive amount of heterogeneous information efficiently from the IoT environment through the Cloud Computing techniques and data mining (DM) technique.DM in IoT plays a critical role in handling heterogeneous data, processing massive amounts of data quickly, providing better analysis, and managing data.

Table 2. Summary of IOT challenges

Author	Research Focus	Challenges	Solutions
(Leal & Atzori. 2010).	Networking	How to secure the network	Mobile Adhoc Network also called as wireless Adhoc network
(Misra et al., 2010).	Routing	How to secure data while transmitting it, and ensure itsdelivery even in case of fault	cross-layered, and Learning automates (LA) basedfault-tolerant routing protocol
(García et al., 2014).	Heterogeneity	How to improve interaction between heterogeneous IOT devices	Midgar Software
(Ali et al., 2015).	Interoperability	How to implement IOT architecture, and facilitate away of accessing information	Semantic Interoperability Architecture
(Ming et al., 2013).	Quality of service (QOS)	How to ensure that performance of services is delivered with high quality	BT, IP & GA algorithm
(Gubbi et al., 2013).	Scalability, and Availability	How to construct scalable architectures which able to handle large bound of requests,provide efficient data processing, and management	cloud computingprivate cloud public cloud Hybrid cloud
(Alam et al., 2010).	Virtualization	How to enhance performanceof IOT structure, and its work	IOT Virtualization Framework based on SenaaS (Sensor-as-a-Service) technology.
(Liu et al., 2015).	Big Data	How to handle, and process huge amount of heterogeneous data efficiently	Cloud Computing. Data mining
(Schulz et al., 2017).	Architecture and Design	How to design adaptivearchitecture	Use of adaptive and context-aware architecture. Cloud computing. Ad-Hoc networks.
(Ray et al., 2014).	Security and privacy	How to maintain privacy, and security to protect data in IOT environment from authorized use.	Use of encryption, use of secure protocol, use of firewall, IDS, IPS use of privacy policies,
(MANGO et al., 2016).	Power consumption	How to reduce power consumption when using IOTconnection	Micro battery technologies

In (Schulz et al., 2017) present efficient guidelines for designing adaptive IoT architecture by integrating various technologies as ad hoc network, cloud computing, adaptive and context-aware architecture. Context-aware architecture plays critical role on process of understanding data, and deciding which data obtained from sensors need to be processed more than other which make system more flexible. In (Ray et al., 2014), the researchers illustrate the best approaches to overcome privacy and security challenges in the IoT environment. They try to maintain high privacy and increased security to protect data from unauthorized use or accesses through integration of new innovative techniques like the use of encryption, secure protocol, firewall, IDS, IPS, and privacy policies. In (MANGO et al., 2016)., the authors offer a general overview of potential technologies that assist in reducing power consumption when using IOT connection, such as integration of Micro battery technologies in IoT environment. Recent development in IoT Micro batteries helps to provide the needed power to continue working under the great requisition of power.

8. Reasons for adapting IOT

Different recent researches find that deployment of IoT systems will encounter various challenges and serious security matters. Nevertheless, they state that if IOT construction copes adequately through integrating appropriate information and communication technologies into the IoT environment, these challenges can be mitigated and restricted effectively (Sahraoui & Bilami, 2014; Nardelli et al., 2017). Several reasons lead most businesses and worldwide organizations to board around this technology, as illustrated in Figure 4. According to the chart, the following chart demonstrates the major motives for adopting IoT in a business environment and, according to the chart, improving, enhancing service qualities or products from the highest reason for the utilization of IoT, which take like 47% of their priority (Sahraoui & Bilami, 2014; Nardelli et al., 2017). It can see that the second significant motive for implementation of IoT in a majority of businesses is to improve the productivity of industries as well as maximize the reliability of operations which form respectively as 45%, 44% of their goals (Sahraoui & Bilami, 2014; Nardelli et al., 2017).

Another important reason for adopting IoT is to reduce possibilities of theft or loss of trade secrets or sensitive information through maintenance of the secure network or secure business framework, and its form as 22%. Overall, most of the businesses recently are boarding into IoT to obtain high revenues via delivering a massive amount of demanded services for individuals. At the same time, consume the lowest cost for purchasing essential material and

less consumption of resources through exploiting the presence of new information and communication technologies (Sahraoui & Bilami, 2014; Nardelli et al., 2017).

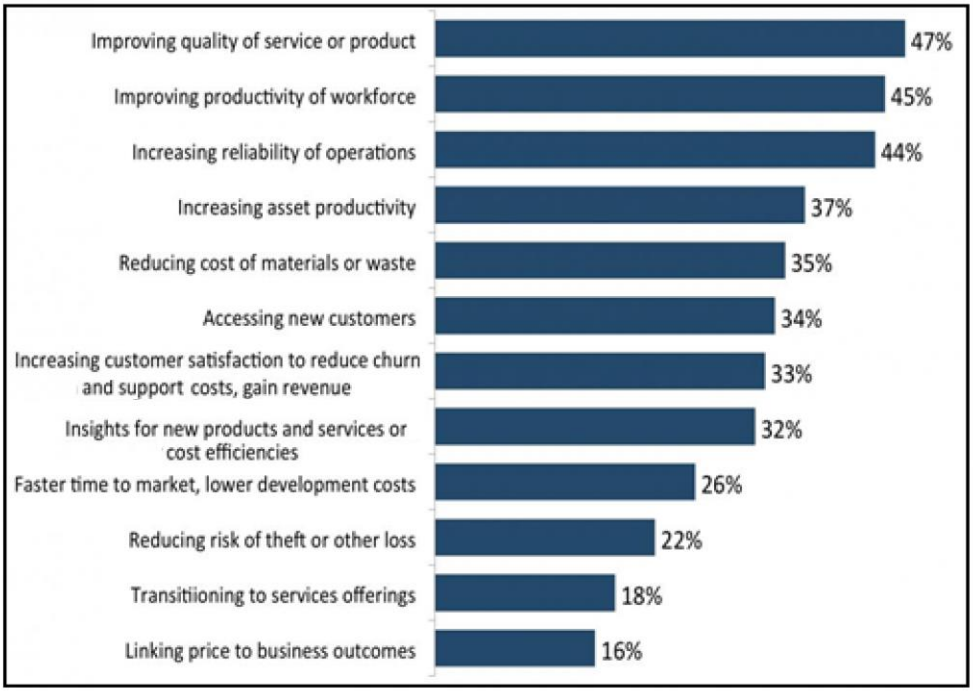

Figure 4. Business reasons for adapting IOT (Sahraoui & Bilami, 2014; Nardelli et al., 2017).

9. Conclusion

This review paper focus on the fundamental idea of IoT that is used to embed various sensors into smart devices to gather required information and then react based on analysis of that information. This procedure will involve three essential phases: collect data through the sensor, transfer data to be analyzed either locally or in the cloud, and finally perform actions. Typically, the perception layer, network layer, and application layer form significant layers to construct IoT architecture. Each of these layers may face different attacks due to security gaps. However, there are various available tools to prevent attackers from breaching security. Maintaining high confidentiality, integrity, availability, and authentication in an IoT environment will serve successful and secure communication among IoT devices. Although boarding into IOT will raise severe challenges, including extensive data management, availability, interoperability, cost but still numerous organizations are directed to deploy IoT for many reasons. The results show that the big reasons for adopting IoT are improving, enhancing service qualities

or products with 47% of their priority. Also, to enhance the productivity of industries and maximize operations reliability, which records respectively as 45%, 44% of their goals. Another important reason for adopting IoT is to reduce possibilities of theft or loss of trade secrets or sensitive information through maintenance of the secure network or secure business framework, and its form as 22%.

Acknowledgment

The research leading to these results has no Project Grant Funding.

References

[1]. Abomhara, M., & Køien, G. M. (2014, May). Security and privacy in the Internet of Things: Current status and open issues. In 2014 international conference on privacy and security in mobile systems (PRISMS), pp 1-8. IEEE.
[2]. Alam, S., Chowdhury, M. M., & Noll, J. (2010, November). Senaas: An event-driven sensor virtualization approach for internet of things cloud. In 2010 IEEE International Conference on Networked Embedded Systems for Enterprise Applications, pp 1-6. IEEE.
[3]. Ali, Z. H., Ali, H. A., & Badawy, M. M. (2015). Internet of Things (IOT): definitions, challenges and recent research directions. International Journal of Computer Applications, 975, pp 8887.
[4]. AL-Balushi, A. I., Yousif, J., & Al-Shezawi, M. (2017). Car accident notification based on Mobile cloud computing. International Journal of Computation and Applied Sciences IJOCAAS, Vol 2 (2).
[5]. AlKishri, W., & Al-Bahri, M. (2021). Expert system for identifying and analyzing the IoT devices using Augmented Reality Approach. Artificial Intelligence & Robotics Development Journal, pp 43-57.
[6]. Al-Shezawi, M. O., Yousif, J. H., & AL-Balushi, I. A. (2017). Automatic attendance registration system based mobile cloud computing. International Journal of Computation and Applied Sciences, 2(3), pp 116-122.
[7]. Atzori, L., Iera, A., Morabito, G., & Nitti, M. (2012). The social internet of things (sIOT)– when social networks meet the internet of things: Concept, architecture and network characterization. Computer networks, 56(16), pp 3594-3608.
[8]. Farahani, B., Firouzi, F., & Luecking, M. (2021). The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions. Journal of Network and Computer Applications, 177, pp 102936.
[9]. FNH Alattar, A Azeez. (2021). Design and Implementation of an Energy Meter System for Optimized Cost using Internet of Things (IOT) Technology, Applied Computing Journal 1 (1), pp 55-65.
[10]. Fortino, G., Guerrieri, A., Russo, W., & Savaglio, C. (2014, May). Integration of agent-based and cloud computing for the smart objects-oriented IOT. In Proceedings of the 2014 IEEE 18th international conference on computer supported cooperative work in design (CSCWD), pp. 493- 498. IEEE.
[11]. IoT-analytics, (2021), State of the IoT 2020. Online [Accessed 14 April 2021] https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/
[12]. García, C. G., G-Bustelo, B. C. P., Espada, J. P., & Cueva-Fernandez, G. (2014). Midgar: Generation of heterogeneous objects interconnecting applications. A Domain Specific Language proposal for Internet of Things scenarios. Computer Networks, 64, pp 143-158.
[13]. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IOT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), pp 1645-1660.
[14]. Leal, B., & Atzori, L. (2010). Objects communication behavior on multihomed hybrid ad hoc networks. In The Internet of Things, pp. 3-11. Springer, New York, NY.
[15]. Liu, C., Yang, C., Zhang, X., & Chen, J. (2015). External integrity verification for outsourced big data in cloud and IOT: A big picture. Future generation computer systems, 49, pp 58- 67.
[16]. Leo, M., Battisti, F., Carli, M., & Neri, A. (2014, November). A federated architecture approach for Internet of Things security. In 2014 Euro Med Telco Conference (EMTC), pp. 1-5. IEEE.
[17]. Magno, M., Spadaro, L., Singh, J., & Benini, L. (2016, June). Kinetic energy harvesting: Toward autonomous wearable sensing for Internet of Things. In 2016 International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM), pp. 248-254. IEEE.
[18]. Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015, December). 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. IEEE.

[19]. Marwedel, P. (2021). Embedded system design: embedded systems foundations of cyber-physical systems, and the internet of things, p. 433. Springer Nature.
[20]. Ming, Z. H. O. U., & Yan, M. A. (2013). QoS-aware computational method for IOT composite service. The Journal of China Universities of Posts and Telecommunications, 20, pp 35- 39.
[21]. Misra, S., Gupta, A., Krishna, P. V., Agarwal, H., & Obaidat, M. S. (2012, April). An adaptive learning approach for fault-tolerant routing in Internet of Things. In 2012 IEEE Wireless Communications and Networking Conference (WCNC), pp 815-819. IEEE.
[22]. Nardelli, M., Nastic, S., Dustdar, S., Villari, M., & Ranjan, R. (2017). Osmotic flow: Osmotic computing& IOT workflow. IEEE Cloud Computing, 4(2), pp 68-75.
[23]. Ray, B. R., Abawajy, J., & Chowdhury, M. (2014). Scalable RFID security framework and protocol supporting Internet of Things. Computer Networks, 67, pp 89-103.
[24]. Raut, N. B., Yousif, J. H., Maskari, S. A., & Saini, D. K. (2011). Cloud for pollution control and global warming. In Proceedings of the World Congress of Engineering, UK (Vol. 9).
[25]. Roman, R., Najera, P., & Lopez, J. (2011). Securing the internet of things. Computer, (9), 51-58.
[26]. 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), pp 2266-2279.
[27]. Schulz, P., Matthe, M., Klessig, H., Simsek, M., Fettweis, G., Ansari, J., & Puschmann, A. (2017). Latency critical IOT applications in 5G: Perspective on the design of radio interface and network architecture. IEEE Communications Magazine, 55(2), pp 70-78.
[28]. Saini, S. L., Saini, D. K., Yousif, J. H., & Khandage, S. V. (2011, July). Cloud computing and enterprise resource planning systems. In Proceedings of the world Congress on Engineering,Vol. 1, pp 681-684.
[29]. Sahraoui, S., & Bilami, A. (2014, May). Compressed and distributed host identity protocol for end-to-end security in the IOT. In 2014 International Conference on Next Generation Networks and Services (NGNS), pp. 295-301. IEEE.
[30]. Statista, (2021). Global-industrial-internet-of-things-market-size. Online [Accessed 14 April 2021] https://www.statista.com/statistics/611004/global-industrial-internet-of-things-market-size/
[31]. Yousif, J. H., & Alattar, N. N. (2017). Cloud management system based air quality. International Journal of Computation and Applied Sciences (IJOCAAS), 2(2).
[32]. Yousif, J. H., & Saini, D. K. (2013). Cloud computing and accident handling systems. International Journal of Computer Applications, 63(19).