Internet of Things Applications and its Security

Hanaa F. M.
Imam Abdulrahman Bin Faisal University, Faculty of Science and Humanities, Jubail

Entesar H. I.
Faisal University, Faculty of Science
Mathematics department

Azza A. A.
Imam Abdulrahman Bin Faisal University, Faculty of Science and Humanities, Jubail

ABSTRACT
Internet of Things (IoT) aims to integrate seamlessly both physical and digital worlds and makes up a new intelligent era of Internet. This technology offers a huge business value for organizations and provides opportunities for many existing applications such as healthcare, smart cities, smart grids, smart building, transportation, and in industrial manufacturing. Security of IoT is very critical issue, so in this paper, number of IoT systems, such as smart healthcare, smart transportation, smart city, and smart manufacturer are explained, also their security requirements are discussed.

Keywords
IoT, M2M, security service.

1. INTRODUCTION
World of smart environments such as smart transports, smart cities and many other areas more intelligent is the specific mean of internet of things (IoT). IoT concept was first proposed in the late 1990s. People can interact with each other or with machines through internet, also machines can interact with other machines through internet. IoT is an idea and a worldview that thinks about unavoidable nearness in the earth of an assortment of things/questions that through remote and wired associations and one of a kind tending to plans can interface with each other and participate with different things/items to make new applications/administrations and achieve shared objectives. IoT communication comes from embedded sensor systems used in industrial machine-to-machine (M2M) communication [4][5]. IoT contributes essentially to improve our day by day life all through numerous applications originate from various areas, for example healthcare, smart cities, smart grids, smart building, transportation, industrial manufacturing among others.

Protection of associated systems in the IoT is very important. The idea of networking appliances and other objects is relatively new, and security has not always been considered in product design.

They are basic three layer that operates IoT [1][2][3] Perception, Network, and Application. The architectural framework of IoT layers is shown in Fig.1. The perception layer function is collecting the data from the environment, with help of sensors and actuators, and then transmitting the data after processing to the network layer [3]. The network layer contains cloud-computing platforms, internet gateways, switching, and routing devices etc. The network layer serves the data transmission to different IoT hubs and devices over the internet. The network gateways serve as the mediator between different IoT nodes by aggregating, filtering, and transmitting data to and from different sensors [3]. Finally, the application layer guarantees the authenticity, integrity, and confidentiality of the data. At this layer, the purpose of IoT or the creation of a smart environment is achieved.

Security services are covered at section.2. Section.3 covers IoT applications and its security Features. Conclusion and future works are introduced at section.4

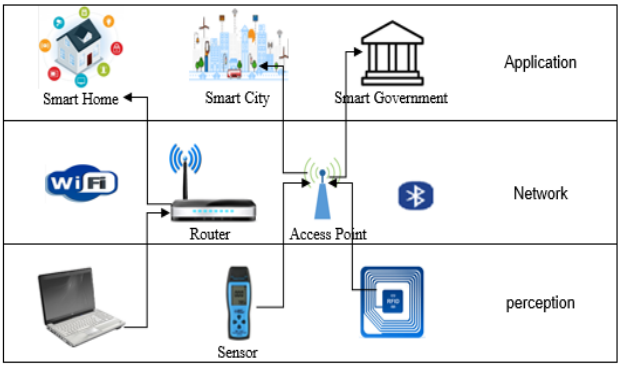

Figure 1. Three-layer IoT Architectures

2. BACKGROUND ABOUT SECURITY SERVICES
The security of computer networks and information systems in general, consists to provide the following services [9]:

Data Confidentiality: Data confidentiality such as encryption and sign-encryption is used to protect data from unauthorized users. The cryptographic mechanisms is classified two types. The first type is symmetric cryptographic mechanisms such as AES and DES, and asymmetric mechanisms such as RSA algorithm, digital signature, identity based encryption (IBE)[12] and attribute based encryption (ABE) algorithms.

Data Integrity - assurance that data received is as sent by an authorized entity. Hash functions, message signature provide data integrity. Message Authentication Code such as HMAC, CBC-MAC, ECDSA algorithms provides data integrity.

Availability- It ensures that the services of the system should be available for legitimate users. Pseudo-random frequency hopping, Access control, Intrusion prevention systems, firewalls provide availability.

Authentication - assurance that the communicating entity is the one claimed. Chain of hash, Message Authentication Code provide authentication.

Non-Repudiation - protection against denial by one of the parties in a communication. Also it said to be Message Authentication Code (MAC).

3. IOT SECURITY CHALLENGES
The security challenges of IoT require the capacity to guarantee security by confirmation, privacy, end-to-end security, respectability and so on. Security implemented in IoT all through the advancement and operational lifecycle of all IoT gadgets and center points [3]. Figure.2 shows the security requirements for IoT. Given beneath are the security services and how it can be achieved in IoT[8].

1) Confidentiality

In IoT a user can be human, machines and services, and internal objects (devices that are part of the network) and external objects (devices that are not part of the network). For example, it is crucial to make sure that sensors don't reveal the collected data to neighboring nodes [5]. One more confidentiality issue that must be addressed is how the data will be managed. It is important for the users of IoT to be aware of the data management mechanisms that will be applied, the process or person responsible for the management, and to ensure that the data is protected throughout the process [6].

2) Integrity

The IoT is based on exchanging data between many different devices, which is why it is very important to ensure the accuracy of the data; that it is coming from the right sender as well as to ensure that the data is not tampered during the process of transmission due to intended or unintended interference. The integrity feature can be imposed by maintaining end-to-end security in IoT communication. The data traffic is managed by the use of firewalls and protocols, but it does not guarantee the security at endpoints because of the characteristic nature of low computational power at IoT nodes.

3) Availability

The vision of IoT is to connect as many smart devices as possible. The users of the IoT should have all the data available whenever they need it. However data is not the only component that is used in the IoT; devices and services must also be reachable and available when needed in a timely fashion in order to achieve the expectations of IoT.

4) Authentication

Each object in the IoT must be able to clearly identify and authenticate other objects. However, this process can be very challenging because of the nature of the IoT; many entities are involved (devices, people, services, service providers and processing units) and one other thing is that sometimes objects may need to interact with others for the first time (objects they do not know) [7]. Because of all this, a mechanism to mutually authenticate entities in every interaction in the IoT is needed.

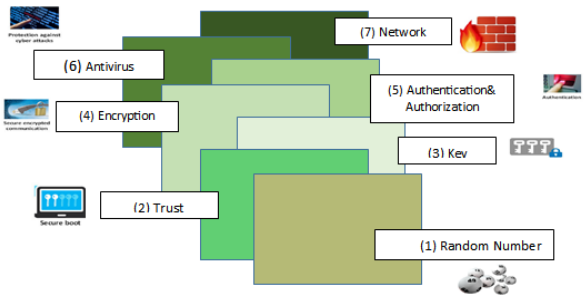

Figure.2. Internet of Things (IoT) Security Seven Layers Structures

4. IOT APPLICATIONS AND THEIR SECURITY REQUIREMENTS

4.1 Smart healthcare

Smart healthcare services assumes a huge part in social insurance applications through implanting sensors and actuators in patients' bodies for observing and following purposes. IoT is utilized as a part of medicinal services so as to screen physiological statuses of patients. The implanted sensors can gather data straightforwardly from the body territory of the patient and transmit it to the doctor. This innovation can possibly totally separate the patient from the unified framework which is the healing facility while keeping up ceaseless contact with the doctor. As of now, Healthcare based IoT applications speak to one of the promising advancements that effect enormously the general public which is predominantly because of the maturing of the populace. In this setting of populace maturing and the cost identified with the treatment, an extraordinary intrigue develops to embrace new IoT based advancements to screen the patients continuously. The security consideration of smart healthcare are listed in three points:

1. Authentication: The entrance to Personal Health Record identified with every patient must be secured against non-approved people, just doctors and medical attendants can get to these records.
2. Confidentiality and Integrity: It's obligatory to secure interchanges amongst patients and doctor's facilities by guarantee classification and respectability of traded information.
3. Privacy concerns: Patients should know, continuously, who possesses and controls their PHRs. Furthermore, it's important to shroud IoT gadgets' areas, patients' personalities, and so on.

4.2 Smart cities

Smart cities consists of the most critical applications of IoT. In this specific circumstance, sensors are conveyed all over streets, building, smart cares, and so on to better oversee activity, adjust to the climate, lighting takes after the situation of the sun, local occurrences can be maintained a strategic distance from with alerts, and so on. Security prerequisites

1- Confidentiality of data and access control of delicate information.

2- Authentication of clients and data's sources.

3- Integrity of information is likewise imperative as these pieces of information are delicate and take an interest in basic leadership what's more, upgrade the day by day life of nationals in the keen urban communities.

4- Availability of data for clients and chiefs.

4.3 Smart transportation

Smart transportation system (STS) means that transportation can connect individuals, streets and smart vehicles using its communication embedded systems. In STS, smart distributed processors is embedded inside vehicles to make the transportation secure, and more helpful. STS utilizes four fundamental segments: Vehicle subsystem, Station subsystem (roadside hardware), ITS observing focus, and security subsystem [10]. In [11], interchanges in vehicular systems is classified as V2V (Vehicle to Vehicle), V2I (Vehicle to Infrastructure), and V2P (Vehicle to Pedestrian). Vehicular security networks concerns with authentication requirement to authenticate senders of messages, privacy and Non-repudiation of drivers to be protected against unauthorized observers, and availability of vehicular networks to be persisted against jamming attacks.

4.4 Industrial manufacturing

These days, IoT assumes a critical part in the business. It is considered as a promising answer for computerize the procedure of assembling and the control of the generation chain. Industrial internet of things (IIoT) utilizes new innovations such as machine-to-machine (M2M) correspondence, Wireless sensor networks (WSN), mechanization advances and in addition big information to make a wise mechanical biological system [11]. The primary point of IIoT is to give better profitability, effectiveness, unwavering quality and better control of conclusive items. IIoT systems claim the following important security requirements:

1- Availability of the system even under critical situations. Deployment of DoS countermeasures maintains the availability of the system.

2- Integrity: Reliability of information to prevent any failure or physical damage.

3- Confidentiality: to protect data, code, system configurations by using encryption mechanisms. Manufacturing process is very secret and sensitive against espionage attacks.

4- Authentication: In manufacturing systems, some production tasks are outsourced to third parties. Therefore, it's mandatory that these third parties must be authenticated and prove its trustworthiness.

5. CONCLUSION AND FUTURE WORK

This paper covered number of IoT systems, such as smart healthcare, smart transportation, smart city, and smart manufacturer and their security requirements. In the future work, we will try to solve the security problem of the transportation IoT application.

6. REFERENCES

[1] K. Zhao and L. Ge, "A survey on the internet of things security," in Int'l Conf. on Computational Intelligence and Security (CIS), 663-667, 2013.

[2] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization," Computer Networks, vol. 56, 3594-3608, 2012.

[3] M. Leo, F. Battisti, M. Carli, and A. Neri, "A federated architecture approach for Internet of Things security," in Euro Med Telco Conference (EMTC), 1-5, 2014.

[4] M. Rouse, "IoT security (Internet of Things security)," IoT Agenda, 01/11/2015.

[5] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (iacac) for the internet of things," J. of Cyber Security and Mobility, vol. 1, 309-348, 2013.

[6] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," Computer, vol. 44, 51-58, 2011.

[7] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, 2266-2279, 2013.

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

[9] H. Noura. Adaptation of Cryptographic Algorithms According to the Applications Requirements and Limitations : Design, Analyze and Lessons Learned. HDR dissertation, UNIVERSITY of PIERRE MARIE CURIE -Paris VI, 2016.

[10] Y. Leng and L. Zhao. Novel design of intelligent internet-of-vehicles management system based on cloud-computing and internet-of-things. In Proceedings of 2011 International Conference on Electronic Mechanical Engineering and Information Technology, volume 6, pages 3190– 3193. IEEE, Aug 2011.

[11] M. Tilal and R. Minhas. Effects of jamming on ieee 802.11 p systems. Master's thesis, Chalmers University of Technology, Göteborg, Sweden, November 2010.

[12] Ali Meligy ; Azza A. Abdo ; Ayman Alazab,"P2P Social Network with Dynamic Identity-based Broadcast Encryption using Rolls", International Journal of Computer Applications (0975 – 8887) Volume 102– No.6, September 2014.