International Journal of Advances in Electronics and Computer Science, ISSN: 2393-2835 Volume-4, Issue-9, Sep.-2017
http://iraj.in

INTERNET OF THINGS (IOT) AND SECURITY ISSUES

SAFAK DURUKAN-ODABASI

Department of Computer Engineering Istanbul University Istanbul, Turkey
E-mail: sdurukan@istanbul.edu.tr

Abstract— Internet of Things (IoT) technology is an emerging concept which presents a connected world with billions of objects, people or devices. Huge amount of data and traffic delivered from these objects makes security and privacy mechanisms necessary. Besides, analysis of the requirements for security and privacy aspects is important to prevent system failures and provide quality of service. In this study, architecture and typical applications of IoT, and an overview of security and privacy concerns are presented.

Index Terms—Internet of Things; IoT applications; IoT architecture; security; privacy.

I. INTRODUCTION

Internet of Things (IoT) is a system that consists of various objects, services, humans and devices which communicate and share data and information to serve for a common purpose and connect real-world and cyberspace. echnological developments are affected by demands of users. Besides, continuity of connection becomes an important desire in our days. Therefore, studies are focused on "Future Internet" that provides an "always connected" model to users [1]. IoT is one of the concepts associated with this model. Structure of IoT in which real-world objects are a part of Internet, they all have unique addresses and permissions to access network, their locations and status are known, is a combination of digital and physical worlds. All of the advantages came along with IoT enable this technology to have an important place among networking technologies.
This work presents an overview of Internet of Things, architecture and applications of IoT, security challenges. The rest of the paper is organized as follows. Section II presents main characteristics and Architecture of IoT. In Section III, the application areas of IoT are referred. Security issues are explained in Section IV and Section V concludes the study.

II. CHARACTERISTICS AND ARCHITECTURE OF IOT

IoT concept needs encoding of physical world as digitally. Therefore, objects must be equipped with computing and communication skills. The boundaries of Internet technologies become expand with decrease of Internet connectivity costs and development on device processing and storage capabilities [2],[3]. Besides, device sizes become smaller and thus, placing various types of sensors on devices is possible. In this way, small devices equipped with sensors can connect and communicate over Internet. The concept of IoT is shown in Fig. 1.

This work was supported by Scientific Research Projects Coordination unit of Istanbul University. Project number: BEK-2017-25558

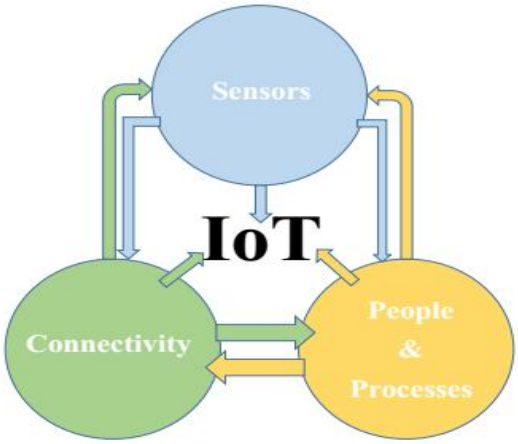

Fig. 1. The Concept of IoT

The main parts of IoT are RFID systems and sensor networks [4]. In RFID (Radio-Frequency IDentication) systems [4],[5] every object has a unique IP that identifies this object to others. RFID consists of unique labels and readers which are able to read these labels. On the other side, sensor networks comprise of nodes with sensing skills and these networks can work compatible with RFID systems.
Combination of physical objects equipped with RFID, NFC (Near Field Communications) tags, electronic bar codes and smart devices which can scan these objects by their RFID/NFC readers, provides a connection between physical world and cyberspace and can be called as IoT [1].
The main characteristics of IoT can be classified as follows:

- Event driven architecture: IoT can be called as an event driven architecture since it is the production, detection, consumption of, and reaction to events.
- Ambient intelligence: IoT has intelligence entities and these entities have abilities like auto-organizing, interoperability and acting independently to answer requirements of the system.
- Complex system: IoT is a complex system due to the huge number of objects, links and interactions between them.
- Semantic sharing: IoT objects must understand each

other to communicate. So, there is need for a semantic sharing mechanism.

- Size, time and space considerations: Since IoT system has ability to encode and track trillions of objects; it must handle billions of parallel and simultaneous events. Therefore, time cannot be used as a linear dimension. Geographic locations are important information for IoT and searching of things is based on their location instead of keywords in such systems.

The "thing" term in IoT concept includes every kind of physical object like smart phones, tablets, smart watches, smart TVs etc. The simultaneous connection to Internet and providing data, information and services by these "things" have transformed "anytime, anywhere for anyone" concept of next generation networks into "anytime, anywhere to anything" [2].

Complex structure of IoT results in huge amount of data to be handled which causes challenges on privacy and security issues [6]. Design of new architectures and protocols is needed to deal these problems.

The layers of IoT architecture are referred based on their functionalities and containing devices [7]. IoT's architecture can be divided into sensor, network and application layers [7],[8] as seen in Fig. 2.

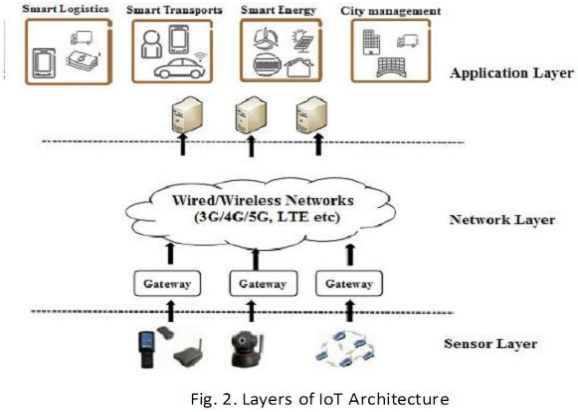

Fig. 2. Layers of IoT Architecture

Fig. 2. Layers of IoT Architecture

Sensor layer consists of various types of sensors. These sensors are in charge of sensing, collecting and processing of data. Also, it transmits data to the network layer.

Network layer plays a role in transferring data which is received from sensor devices, to the central processing unit safely. Cloud, Internet gateways and routers are operated by using next generation networks like Wi-Fi and LTE [8].

In application layer, data integrity and authorization processes are performed. Application management is handled in this layer. The IoT applications can be smart logistic, smart transport, smart energy, smart health, smart home, etc.

III. APPLICATION AREAS OF IOT

Application areas of IoT are limited just with imagination and budget. From healthcare applications to logistic, IoT becomes a part of our lives. In Fig. 3 most popular IoT applications are represented.

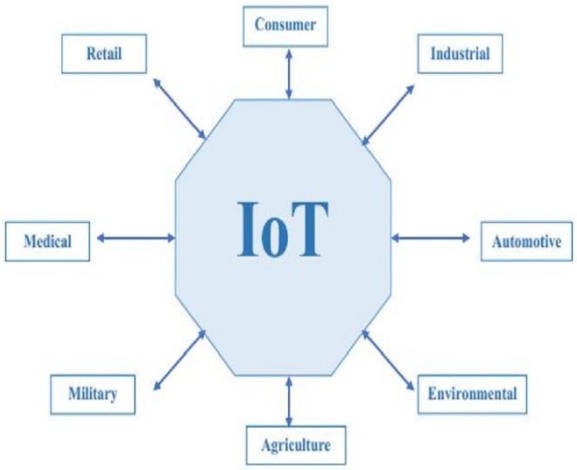

Fig. 3. IoT Applications

In [9], IoT applications are divided into 14 groups as transportation, smart home, smart city, lifestyle, retail, agriculture, smart factory, healthcare, culture, environment and energy, supply chain, emergency and user interaction. However, there are six key markets for the IoT with potential for exponential growth according to recent researches [10],[11],[12]:

1. Building and Home automation

Smart home/building idea is proposed in early 1990 and has an important place in IoT technologies. Smart home/building technology and automation are based on human-computer interaction and makes devices control remotely. In this way, an intelligent home/building management and comfortable living environment are provided to users. Besides automatic switching off some electrical equipment like air condition, TV, light bulb etc. when they are not in use, could reduce the cost

2. Smart Cities

Growth on the population of people who live in the cities and accordingly increment on the complexity of analyzing data, solving problems and coordination of the sources effectively are the Smart City concept's point of the origin. The goal of building a smart city is to improve quality of residents' life and provide their needs by using efficient services. In a smart city, authorized people can interact directly with the community and the city infrastructure and monitor what is happening in the city and thus, they can decide which changes are needed to improve quality of life.

3. Smart Manufacturing

Traditional methods are not sufficient to increase productivity on manufacturing anymore. As a result, new solutions namely smart manufacturing has been presented and from supplier to end consumer whole production chain became integrated with digital systems. Smart manufacturing reduces the cost because it enables all information about the manufacturing process to be available when or where

it is needed.

4. Wearable Technologies

It can be said that wearable technologies are the biggest innovations since smartphones. A wearable technology is more than a gadget which a person can wear. It is also a device that incorporates a computer and advanced electronic technologies to exchange data with a manufacturer, operator or other connected devices by using embedded sensors and actuators. There are various kinds of wearable technologies like smartwatches, fitness trackers, sports watches, head-mounted displays, smart clothing, smart jewelry and implantable.

5. Healthcare Systems

IoT is used for healthcare domain widely by the day to improve access to care, increase the quality of care and reduce the cost of care. Data collected from medical devices requires follow-up interaction with a healthcare professional for some patients. Internet-connected devices fill this gap and ensure the interconnection between patient and the professionals.

6. Transportation

Application of IoT consists of transportation systems' all aspects like the vehicle, the infrastructure, and the driver. In recently, public transportation is used more frequently by people. As a consequence, organizations are looking for solutions to improve their service against traffic congestion, pollution problems and transportation of goods and people in a safe manner. Interaction between components of transportation systems provides inter and intra vehicular communication, smart traffic control, smart parking, electronic toll collection systems, logistic and fleet management, vehicle control, and safety and road assistance.

IV. SECURITY AND PRIVACY ISSUES ON IOT

IoT faces with important security and privacy challenges. IoT devices can be used either for providing and endangering security and privacy of a system [4]. Besides, the architecture of IoT in which billions of objects are connected and interact, renders security and privacy violation attractive [14]. Also every device of this architecture is a potential entrance to infiltrate into the system and access personal information.

The most important difficulty in the systems which have dynamic and flexible structures like IoT is to detect the requirements of security and privacy. There are some questions to be answered while analysing of system security and privacy: "When and whom the information must be protected from?". Also, IoT is affected all security and privacy threads of the consisting technologies of IoT.

Fig. 4 shows the main aspects that must be taken into consideration to specify security issues in an IoT system.

IoT architecture can be divided into 4 layers as sensing, network, service and application-interface according to security requirements [15]. Each layers' security needs are different because of their features. Solutions aimed to solve security problems of an IoT system must consider all of these

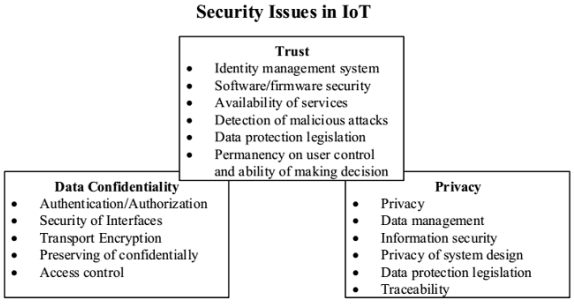

Fig. 4. Security Issues in IoT [15]

layers' requirements besides the security requirements between layers and the security requirements for services.

Access control, authorization and authentication must be performed properly to overcome all of these problems on IoT systems [1]. Access control mechanisms are responsible for identifying who can access the system resources, what are the limits of the user and its access.

The first step of this process is identification of IoT elements and systems like EPC (Electronic Product Code) [16] and IdM (Identity Management) [17],[18]. Authentication mechanism ensures providing confidence between different objects, people or systems before setting a communication channel by identification. Authentication mechanisms can be grouped as central and peer to peer. Kerberos [19] is an example of central mechanisms while [20] is a peer to peer one.

Authorization is entitled to license, restrict or prevent of the access of data, resource or applications in an IoT system. RBAC (Role-Based Access Control) [21] is a method to be used for management on online systems that have multi-users and applications.

Security concerns on IoT can be classified as follows [1]:

• Sensors and Equipment: In a typical IoT architecture, it is open to attack since some part of sensors and devices are destitute of tracking systems. End-front sensors and equipment are responsible for receiving data from smart sensors and sending it to central processor unit by using M2M module device. Thus, IoT systems are subject of service attack and eavesdropping.

• Network: In IoT, network plays a part of all M2M communication management and QoS. A large quantity of data sending to heavy traffic networks from large number of devices connected to the network causes denial of service attacks.

• Back-end: Back-end has an important part of IoT because it requires high-security and efficient data analysis of sensors to process real time data. Privacy protection, access control, user authentication, communication security, data integrity, data

confidentiality and availability are the main domains of the typical security of IoT systems [22].

On the other hand, privacy concerns can be grouped as follows [1]:

• Privacy in device: Unsecure devices always open to attacks. Deficiencies on design of software or hardware cause this defenselessness. Cryptology is used to prevent unauthorized access to the system.

• Privacy during communication: Encryption is necessary for privacy conservation of data during communication. In addition, secure communication protocols must be integrated to the system.

• Privacy in storage: Anonymization, pseudonymization techniques and hiding specific record and statistical data can be used to keep information privacy in storage devices.

• Privacy in processing: There are two main problems which cause privacy issues during processing. Firstly, sensitive data must be behaved in an appropriate way. Then, the users who do not know how to prevent privacy and security can express or transfer their personal data accidentally. DRM (Digital Right Management) [22] is one of the effective methods that prevent illegal usage and distribution.

CONCLUSION

IoT gains popularity and, its application area becomes expand day by day. However, improvements are needed to conserve security and privacy of IoT systems to raise the system quality. Analyzing of the requirements for security and privacy is crucial to avoid critical failures on complex systems. Current security mechanisms must be regulated before integrating to the systems. By this way, to open systems against attackers uncontrollably is inhibited. Additionally, defining new architectural standards enhances system security.

IPv6 which has wider identification capacity must be put into use, because IPv4 protocol fails to satisfy for identifying and connecting a huge amount object came with IoT. In addition to all this, security problems of every new included technology become matters that IoT must overcome.

As a result, each layer of IoT has a potential of being under attack. As a consequence, security problems and requirements must be specified efficiently. Although current IoT researches focus on authorization and access control protocols, it is required to cooperate with new protocols like IPv6 and 5G to enable dynamic structure of IoT. Dealing with the issues like security, privacy, authentication and access control, could make a transformation via IoT possible.

REFERENCES

[1] S. Kraijak and P. Tuwanut, "A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends," 2015 IEEE 16th International Conference on Communication Technology (ICCT), Hangzhou, 2015, pp. 26-31.

[2] L. Coetzee, J. Eksteen., “The Internet of Things - Promise for the Future? An Introduction.” 1ST-Africa 2011 Conference Proceedings (CSIR), Gaborone 2011, pp. 1-9.

[3] I. Alqassem and D. Svetinovic, "A taxonomy of security and privacy requirements for the Internet of Things (IoT)," 2014 IEEE International Conference on Industrial Engineering and Engineering Management, Bandar Sunway, 2014, pp. 1244-1248.

[4] L. Atzori, A. Iera, and G. Morabito. “The internet of things: A survey”, Computer Networks, 54(15):2787–2805, Oct. 2010.

[5] [5] M. Buettner, B. Greenstein, A. Sample, J. R. Smith, and D. Wetherall. “Revisiting smart dust with RFID sensor networks.” In Proc. 7th ACM Workshop on Hot Topics in Networks (Hotnets-VII), Calgary, Alberta, Canada, 2008, pp.37-42.

[6] [6] R. Khan. S. U. Khan. R. Zaheer and S. Khan. Future Internet: “The Internet of Things Architecture, Possible Applications and Key Challenges”, 10th International Conference on Frontiers of Information Technology, Islamabad, 2012, pp. 257-260.

[7] [7] 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.

[8] [8] 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.

[9] [9] O. Vermes an, P. Friess, A. Furness. The Internet of Things 2012. By New Horizons. 2012. [Online]. http://www.internet-of-things-research.eu/pdflIERC_Cluster_Book_2012_WEB.pdf

[10] [10] Bandyopadhyay, D., Sen,, “Internet of Things: Applications and Challenges in Technology and Standardization” J. Wireless Personal Communication ,58(1):49-69, 2011.

[11] [11] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Future Gener. Comput. Syst., 29:1645–1660, 2013.

[12] [12] A.Karkouch , H. Mousannif, H. A. Moatassime, T. Noel, “Data quality in internet of things: A state-of-the-art survey”, Journal of Network and Computer Applications, 73: 57–81, 2016.

[13] R. Roman, J. Zhou, and J. Lopez. On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10):2266–2279, 2013.

[14] F. Thiesse, C. Floerkemeier, M. Harrison, F. Michahelles, and C. Roduner. “Technology, standards, and real-world deployments of the epc network”, Internet Computing, IEEE, 13(2):36–43, 2009.

[15] Li, S. Xu, L.D. (2017). Securing the Internet of Things. Cambridge. Syngress Press.

[16] A. Bhargav-Spantzel, A. Squicciarini, and E. Bertino. Trust “Negotiation in identity management”, Security Privacy, IEEE, 5(2):55–63, 2007.

[17] A. Vapen, D. Byers, and N. Shahmehri., “2-clickauth optical challenge response authentication.”, ARES ’10 International Conference, Krakow, pp. 79–86, 2010.

[18] Y. Kirsal and O. Gemikonakli. “Improving kerberos security through the combined use of the timed authentication protocol and frequent key renewal.”, 7th IEEE International Cybernetic Intelligent Systems Conference,London, pp. 1–6, 2008.

[19] G. Chen, H. Chen, L. Xie, G. Song, and T. Zhuang., “An identity authentication scheme in wireless peer-to-peer network”, 12th IEEE International Conference on Communication Technology (ICCT), Nanjing, pp. 473–476, 2010.

[20] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman., “Role-based access control models.” Computer, 29(2):38–47, 1996.

[21] E. WeI bourne, L. Battle, G Cole, K. Gould, K. Rector, S. Raymar, M. Balazinska, G Borriello. “Building the internet of things using RFID: the RFID ecosystem experience.”, IEEE Internet Computing. 13(3): 48-55, 2009.

[22] J. S. Kumar, D. R. Patel. "A Survey on Internet of Things: Security and Privacy Issues", International Journal of Computer Applications. 2014: 20-25

[23] S. Chen, B. Mulgrew, and P. M. Grant, "A clustering technique for digital communications channel equalization using radial basis function networks," IEEE Trans. on Neural Networks, vol. 4, pp. 570-578, July 1993.

[24] J. U. Duncombe, "Infrared navigation—Part I: An assessment of feasibility," IEEE Trans. Electron Devices, vol. ED-11, pp. 34-39, Jan. 1959.

[25] C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, and M. Miller, "Rotation, scale, and translation resilient public watermarking for images," IEEE Trans. Image Process., vol. 10, no. 5, pp. 767-782, May 2001.

★★★