IoT Sistemini Güvenliği: Yeni Bir Model

Securing the IoT System: A New Model

Ahmed Abdulmaged Ismael
Software Engineering Department
College of Technology
Firat University
Elazig, Turkey
ahm.sula@gmail.com

Asaf Varol
Software Engineering Department
College of Technology
Firat University
Elazig, Turkey
varol.asaf@gmail.com

ÖZET

Makale, Nesnelerin İnterneti'ni (IoT) güvenlik açısından ve IoT cihazlarının güvenliğini sağlamada karşılaşılan çeşitli zorlukları analiz etmeyi amaçlamaktadır. Nesnelerin İnterneti (IoT), farklı perspektiflerde incelenmesi gereken günlük bir konudur. IoT'nin başarısı, cihazları yaparken mimariyi ve bileşenin ne kadar verimli ve güvenli olduğuna bağlıdır. Odak noktası, sensörler tarafından son katmana temsil edilen ilk katmandan, IoT'deki tüm fazlara veya katmanlara güvenlik ve gizlilik sağlayarak, IoT'nin saldırılardan ve sızmalardan nasıl korunacağı üzerine olacaktır. IoT cihazlarının en iyi şekilde çalışması için garanti edilmesi gereken farklı katman güvenlik noktaları vardır. Bunlar arasında sensör katmanı güvenliği, arabirim katmanı güvenliği, ağ katmanı güvenliği ve hizmet katmanı güvenliği yer alır. IoT için güvenliği kapsayan temel yönlerden bazıları gizlilik, mahremiyet, özgünlük, feragatname ve kullanılabilirliktir. Son olarak, bu makale, IoT mimari bileşenlerini güvence altına almanın farklı yollarını ele almaktadır.

Anahtar Kelimeler: Bir şeylerin interneti; IoT Güvenliği; IoT Mimarlık; Güvenli IoT için Zorluklar.

ABSTRACT

The paper seeks to analyze the Internet of Things (IoT) from a security point of view and the various challenges encountered in securing IoT devices. Internet of Things (IoT), is an everyday subject that needs to be scrutinized in different perspectives. The success of IoT depends on how efficient and secure the architecture and component are while making the devices. The focus will specifically be on how to protect IoT from attacks and penetrations by providing security and privacy in all phases or layers in the IoT from the first layer, which is represented by sensors to the last layer. Security challenges in these classes will also be addressed. There are different layer security points that must be guaranteed for IoT devices to function optimally. They include, sensor layer security, interface layer security, network layer security, and service layer security. Some of the key aspects that encompass security for IoT include confidentiality, privacy, authenticity, non-disclaimer and availability. Finally, the paper talks about the different ways of securing IoT architectural components.

Keywords: Internet of Things; IoT Security; IoT Architecture; Challenges to Secure IoT.

1. INTRODUCTION

Have you ever imagined that everything in your life can be connected to the Internet? Your clothes, your cars, your home lights or even your tea pots have their own accounts on social networking platforms. Internet and social networks send and receive data between them and to the cloud. The connection also allows data collection from different devices. This is what is known today as IoT, where the signals between the real world and the Internet world are increasing by converting every day's physical devices into intelligent objects linked to each other. Making of smart devices is a great scientific renaissance to production new products and services to improve people's everyday lives. The move results in generation of new interconnectivity works and making enterprises in all fields, factories, roads, air navigation, shops, and public buildings smarter. The interconnection of billions of devices permeate the environment around us including human bodies. This is what is known as the radical transformation of our new and receptive lifestyle [1].

This tremendous development will be defined by two major factors which are security and privacy. It is clear that lack of assurance of privacy results into reduced

dependency among users. A prospective study has shown that digital consumer confidence indicate that it is difficult to trust technical companies when it comes to using their personal data. The recent EU Commission on Internet Governance and recent FTCs have clearly demonstrated that there is an urgent need to apply security measures to minimize the impact of cyber-attacks and to curb malicious individuals. More specifically, "common standards" must be defined by applying a set of security rules or procedures in future by a virtual organization in an operational environment that adopts the regulatory safety policy [1].

2. OVERVIEW OF IOT

IoT is a new generational term of that simply means let's communicate between devices connected to each other via Internet protocols. The concept extends to include everything that can be linked to the Internet, ranging from cars that can be programmed to communicate directly with maintenance centers when a defect is detected, passing through to all the devices of the house that can be controlled remotely when connected to the Wi-Fi [2].

IoT Connection Types are as follows:

Internet Direct Connection

All devices are joined and communicate together over the Internet.

Internet Indirect Connection

All devices are joined and communicate together over the Internet or internally but through IoT gateway.

3. IOT ARCHITECTURE

IoT architecture consists of four main phases as in Fig. 1. The first phase of the IoT architecture related to the network is sensors and their actuators to read signals from the existing climate or thing beneath mensuration and converting it into helpful data. Phase two contains sensor data reading structures and data conversions from analog to digital data by aggregating this datum and converting it to digital flows [3].

When the analog conversion phase is complete, the Internet portal gets the collected and digitized information and processes it over Wi-Fi in connection to the nearby wired systems [3].

When IoT information has been converted and collected, it is prepared to pass into the domain information technology field. However, data might sometimes demand more processing before it is transferred to the data center or cloud systems, which is referred to as the third phase or the edge of information technology systems perform. Finally, in phase four, data that needs more in-depth processing is redirected to the actual datacenter or cloud systems, where the most controlling information technology systems are and can analyze, administrate and store it safely [3]. As shown in below Fig. 1. When IoT information has been converted and collected, it is prepared to pass into the domain information technology field. However, data might sometimes demand more processing before it is transferred to the data center or cloud systems, which is referred to as the third phase or the edge of information technology systems perform. Finally, in phase four, data that needs more in-depth processing is redirected to the actual datacenter or cloud systems, where the most controlling information technology systems are and can analyze, administrate and store it safely [3]. As shown in below Fig. 1.

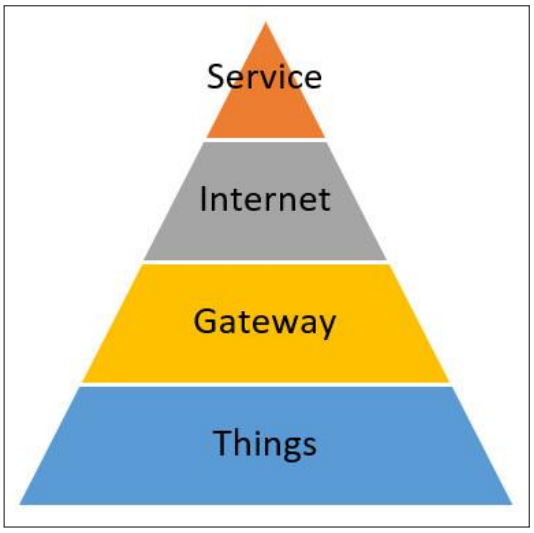

Fig 1. IoT Architecture

4. IOT SECURITY

IoT is the new version of the Internet that merges different types of networks including mobile networks, Internet, social networking, and smart objects to each other to provide new services to users. The success of IoT is largely dependent on enhanced security and privacy at all levels, provision of secure operation, high accuracy and the validation of operations on a large scale. But as the use of IoT increases dramatically in our daily lives and everything around us, the form of threats and attacks on IoT infrastructure is rampant. Therefore, it is essential to take IoT security with seriousness by

analyzing and comprehensively understanding all kinds of possible threats and attacks on the IoT infrastructure [4].

IoT Data Security Challenges

In view of all this information and the promising prospects of a huge growth in this sector, security concerns are increasing. The increasing concern is due to the possibility of not managing and operating of the IoT infrastructure for the functioning and connection of these devices in an optimal and safe manner. This may lead to the possibility of penetrating some of IoT devices and manipulating their artificial intelligence or violation of the privacy of data circulating through them. The security threat might adversely affect the effectiveness of the whole system. In order to achieve a secure and reliable technological future, it is important for cloud computing service providers to assure users that their data and information is adequately protected. This could be achieved by activating all the security precautions and the development of distributed backup plans and disaster recovery speed at all levels, starting from the devices of Internet service providers and their network to access the data center connected to each other on the World Wide Web (www). Then, it could be enhanced by enabling and managing cloud computing infrastructure services to the applications, software, and security algorithms used to build the Internet of Things framework [5].

Fig. 2. illustrates security requirements for a simple Internet framework, where key security requirements are addressed in six aspects:

- Confidentiality - To prevent the disclosure of information to unauthorized persons.
- Integrity -This term refers to trustworthy information, which is created by persons who have the ability to modify or destroy this information.
- Availability - the information system is intended to serve its purpose, where information should be available when needed. This means that system elements work correctly and continuously.
- Non-Disclaimer - The ability of a system to prove that a particular user, not others, has created the information and that the information has not been modified.
- Authenticity - The ability of the system to verify that the information created or modified is the same as that declared by the concerned party.
- Privacy - Maintain personal data from unauthorized use such as adding, deleting, and modifying.

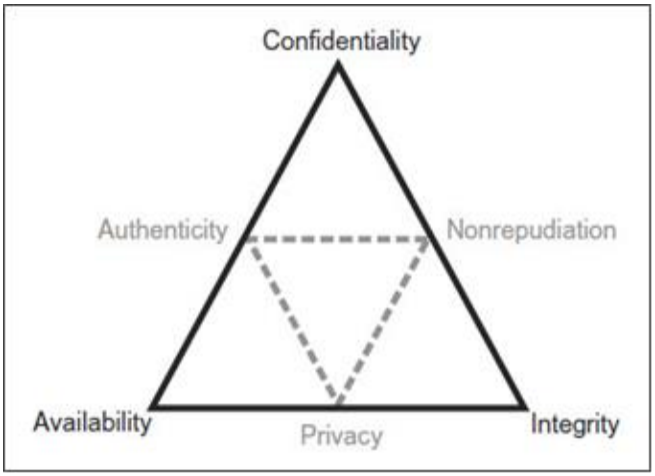

Fig 2. IoT Security.

The key Internet security challenges include the following points the first one is (Data confidentiality) is a term used to conceal information, so that it is made available only to the parties concerned. It is authorized to disclose it or to maintain personal data from theft by using various methods such as encryption and passwords and ensuring data access control and confidentiality. The second one is (Privacy) keeps personal data from unauthorized use such as adding, deleting, and editing. As well as manages information security risks, data protection legislation and illegal processing. And the last one is (Trust) it comes to hardware interconnection, trusting the IoT is one of the most important aspects. Several safety reference points can be focused on, including safety across the various areas of IoT and IoT-EPI projects, which have also been taken into account. The concepts can be used as guiding tools for developing a wide range of Internet applications. The list includes five different categories, trustworthiness, security, transparency, privacy and compliance [6].

Sensor Layer Security

In order to provide security in IoT in an integrated way, the sensors should be designed and integrated into the devices themselves. This means that the process of manufacturing these devices must protect the data to

maintain the safety and limit access to locally stored data in order to keep its privacy [6], [7]. As shown in Fig. 3.

Therefore, the security level of the devices should be high enough to prevent unlawful persons from accessing data stored in them. Also, as Internet devices have been evolving at an accelerated pace in the last ten years, the physical security is very crucial. So, security is vital in designing and manufacturing of resistive IoT devices against manipulation and making them strong at the same time. This makes it hard to read out sensitive information such as personal data, encryption keys or certification [6], [7].

Internet devices are supposed to last for longer time and therefore they should have inbuilt software capabilities. Even with inbuilt software update capabilities, some updates create a loophole for malicious individuals to penetrate and exploit the security vulnerabilities. Therefore, securing IoT devices is a must since the threat of penetration is inevitable [6], [7].

The sensor is a group of devices that are assembled to measure some physical or chemical happening (such as temperature, clamminess, fog, darkness, etc.) and then transferring information to the data processing center to make use of it without the need for physical presence [6], [7].

The sensor node consists of a device that has accurate processing, is able to take a survey, make wireless communication, and may be fitted with a small screen to display the results. However, the device has a small capacity of memory as well as limited energy storage [6], [7].

Fig. 3. Illustrates the sensor components and they are discussed below:

The components include, sensor unit, data processing and storage, and transmitter and receiver unit. Sensor consists of sensors and data conversion from analog to digital system. The main task of this module is to enable data transfer (sent and received) to be adapted to the nature of the data to be used in the processing and storage unit. The storage and processing unit is a microchip with a memory module and data processor that is limited. The transmitter and receiver unit is a unit which consists of a transmitter and receiver of the radio waves via the antenna installed in the device. To add to the aforesaid units, there are three choice units, as follows:

- Detect location unit: it is where the design depends on the sort of practice used and its task is to point out the coordinates of the devices in the observation domain compared to the constant point.
- Mobility unit is applied to free the devices from one area to another according to the need of the network.
- An energy generating unit is the unit responsible for recharging the energy stock of the device.

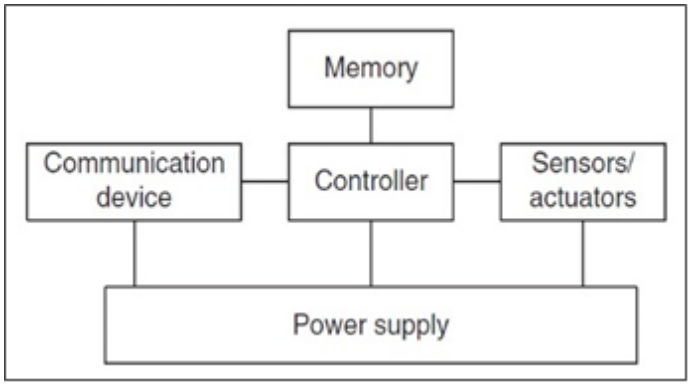

Fig 3. Sensor layer.

Network Layer Security

The architecture of the center network layer is like the design sent in ordinary networks. The function of this layer is to give ways to convey, trade and network information amongst different sub-networks. The main differentiator between IoT and customary center layers is the activity profile. The IoT activity and information might be extraordinary, for instance, interesting conventions and variable parcel estimate. Security administrations at the center network guarantee that the IoT/M2M framework in general has been solidified to guard it against dangers. The following are examples of security concerns for network layers [7].

- Man-in-the-middle (MITM) is the method by which the aggressor can effectively make an association between two points and listen to their discussion by relying on the messages it receives: such as notifications from one companion to the other and concurrently capturing the information.

- Pantomime (spoofing) is the method by which an assailant has traded off a personality and along these lines, through pantomime can send pernicious activity to casualty endpoints on the network.
- Secrecy tradeoff is the method by which the information that is being transferred can be changed by an assailant.
- Replay assault is the method by which legitimate information is retransmitted or postponed by a foe to gain access to an officially settled session by spoofing their own particular personality.

Service Layer Security

This IoT center addresses stages that are particular administrations for gathering information from IoT gadgets. The center also does information handling, and association with different administrations for basic leadership about further exercises, for example, initiating actuators, and so forth. Building up ones' own particular stage requires a big group of individuals and a period of a long time. It is argued that there are more than 300 of them available and that their number keeps increasing. Existing stages have been produced throughout the years, and behind them are expansive groups that have been working on advancement of the stages for about 20 years. The vast majority of the created stages utilize the current framework such as IaaS, PaaS. Along similar lines, some portions of the duties identified with the physical execution of the administration or the execution of the working framework programming are exchanged to others, consequently decreasing the piece of the duty of the group building up its own stage. As to the design of the administration that is being utilized, the REST engineering is overwhelming, while as far as security is concerned, a portion of the cryptographic calculations are utilized, for example, SSL, TLS, AES [7], [8].

Interface Layer Security

It is important to note that the core of the IoT security is in the Interface layer. As the name suggests, it means an Application Interaction Layer. So, Interface layer is nothing but an Application layer and it is a top-level terminal. Mainly, this layer only provides the services for user as per their needs [8].

The functionality of this is that the user can login Air Conditioner or TV or any other device by IoT. During this process, data sharing is a major feature of Interface layer which creates data privacy problems and access control. To overcome these types of access control or data privacy problems, we have to take some measurements in IoT into consideration such as key agreement and authentication across the heterogeneous network, and user privacy protection [8].

The IoT security can be provided at Interface layer with Lightweight encryption technology, secure cloud computing, authentication, and key agreement [8].

Challenges to Secure IoT

Deployment

The deployment of sensors is the first stage in the formation of wireless sensor networks. At this stage, care must be taken in the deployment of these devices so as to meet the objectives. However, the nature of the field in which sensors are to be deployed, as well as the available number of these devices may affect the mode of propagation. In case of access to the field and to locate the sensors, the diffusion of sensors may be carried out manually or using a robot in advance.

In both ways, the responsibility of covering the field and network connectivity and redistribution are left to a sensor. It is clear that the process of deployment poses new challenges.

On the other hand, some fields may be located in hard-to-reach areas, or requires a large number of sensors to be deployed. So, the best way in a deployment strategy may be through the use of modern techniques even though they are costly when compared to the traditional publishing costs.

Energy

Despite the limited capabilities of sensors in terms of processing, storage and communication, the restrictions are expected to be resolved in the near future. However, restrictions on energy consumption seem to pose a new challenge, because of the slow progress in technologies related to battery solutions. The sensors require frequent battery changes, which may be impossible at times. Therefore, efficient energy protocols are necessary to improve the functioning of sensor networks.

Network architecture

If we compare it to traditional networks the structure and the built-in wireless sensor networks differ in many things. For example, there are many operational

characteristics of sensors that can only be known after the completion of their publication and organization. Due to the limited capacity of these devices, many operations must be implemented in parallels, such as monitoring, encryption and data transmission. Due to all these differences, the standard definition of wireless sensor networks is an important task. Also, the wireless sensor networks still rely on the techniques and protocols used in the traditional networking structures.

Degree of reliability

There are many elements to consider when dealing with sensor networks, such as reliability. These networks usually suffer from transmission and reception faults through wave collisions and data packet congestion. In addition, the devices are subject to failure either due to malfunction or interference with the takeover control of these devices. Moreover, there are a lot of details about the type of messages used. They may be in the form of a single package or a set of packages where several packets are sent together in the form of successive packets. These types of messages may require delivery.

Reliability can allow the main station to deliver messages either to all sensors or to a specific group or to a specific area in the observed field. Conversely, all these factors need to be considered when addressing the reliability of wireless sensor networks. Therefore, the development of network reliability protocol takes all these factors and is another challenge in this area.

Programmability

One of the main challenges to be addressed is the capability of devices in wireless sensor networks for programming. This is the case because, the current interface of the sensor requires users to participate in a lot of programming details where they must prepare and process communication between the sensors and determine the methods of aggregation and selection of databases in addition to some other functions.

Network security

Unlike traditional networks, wireless sensor networks are commonly deployed in exposed areas and subject to environmental changes. Sensors are, therefore, susceptible to direct external attacks. Current security techniques and data compression methods are not suitable for use. The devices at the design are not taken as security targets, and as a result, the authentication of the user and confidentiality of data and the adoption of encryption keys and resistance to any kind of attacks on communications impose a new challenge.

Data collection and processing

The sensors are more efficient in processing local data compared to when raw data is transmitted to the main station to be processed. So, a large number of sensors may lead to a flood of messages. To solve this problem, some sensors are selected for purpose of data collection, but the clustering algorithms require storage of messages before processing and this is a major challenge in sensors with low processing capacity and with specific storage spaces.

5. CONCLUSION

It is clear from the paper that security is the major concern for the Internet of Things because automation of people's lives is an inevitable trend. Data privacy and confidentiality in this digital era are some of the key aspects that IoT infrastructure needs to assure IoT users. Big data running into gigabytes is collected every day from the Internet of Things, but the major concern is how this data is stored and used. If the above raised concerns can be adequately addressed, then the Internet of Things is unstoppable and will be fully embraced.

REFERENCES

[1] Ahmed, S.H. and Rani, S., 2018. A hybrid approach, Smart Street use case and future aspects for Internet of Things in smart cities. Future Generation Computer Systems, 79, pp.941-951.

[2] Alaba, F.A., Othman, M., Hashem, I.A.T. and Alotaibi, F., 2017. Internet of Things security: A survey. Journal of Network and Computer Applications, 88, pp.10-28.

[3] Alfaqih, T.M. and Al-Muhtadi, J., 2016. Internet of Things Security based on Devices Architecture. International Journal of Computer Applications, 133(15).

[4] Alkhalil, A. and Ramadan, R.A., 2017. IoT Data Provenance Implementation Challenges. Procedia Computer Science, 109, pp.1134-1139.

[5] Botta, A., De Donato, W., Persico, V. and Pescapé, A., 2016. Integration of cloud computing and internet of things: a survey. Future Generation Computer Systems, 56, pp.684-700.

[6] Ouaddah, A., Mousannif, H., Elkalam, A.A. and Ouahman, A.A., 2017. Access control in the Internet of things: big challenges and new opportunities. Computer Networks, 112, pp.237-262.

[7] Sha, K., Wei, W., Yang, T.A., Wang, Z. and Shi, W., 2018. On security challenges and open issues in Internet of Things. Future Generation Computer Systems, 83, pp.326-337.

[8] Yogita, P., Nancy, S. and Yaduvi, S., 2016. Internet of Things (IoT): Challenges and Future Directions. International Journal of Advanced Research in Computer and Communication Engineering., 5(3), pp.960-964.

ÖZGEÇMİŞ *(LER)*

Ahmed Abdulmaged

He is a master student at Software Engineering of College of Technology at Firat University in Turkey. He is worked in the field of information technology, especially in the field of communications and computer networks. His research interests are Network security and ICT management. He can fluently speak Arabic and English.

Asaf Varol

Dr. Asaf Varol is the Chair of the Software Engineering Department at College of Technology of Firat University in Turkey. He is the founder of the Department of Digital Forensics at Firat University which is first and still unique in Turkey. His research interests are cyber security, robotics, IoT Technologies, Digital Forensics, and Public Administration. He has published more than 300 articles, proceedings, books, etc. He can speak German, English and Turkish.