Internet of Things Security based on Devices Architecture

Taha M. Alfaqih
Information System Department
King Saud University
Riyadh, Saudi Arabia

Jalal Al-Muhtadi
Computer Science Department
King Saud University
Riyadh, Saudi Arabia

ABSTRACT
The Internet of Things, also called The Internet of Objects, refers to a wireless network between objects; usually the network will be wireless and self-configuring, such as household appliances. Secures IOT end-to-end, which means authenticating device communications, protecting code and applications, and securing devices from threats. Emergence accompanied the IoT technology, or when using of this technology and its deployment, an increase in security and privacy violation, so must take caution when used , and also paid to further research in this technology which that bothered a lot, including confidentiality, authenticity, and integrity. In this paper we will present the security and privacy when using the Internet of Things technology, depending on the architecture of the devices, and will be focusing on how security building in the devices, and protection requirements, by studying the architecture layer and IoT security infrastructure.

Keywords
Internet of Things, RFID, GPS, Privacy, authentication.

1. INTRODUCTION
Kevin Ashton first used the term Internet of Things in 1999. The Internet of Things refers to a network of objects, such as household appliances or digital controllers, etc. that uses the networking technologies or backbone of the Internet (TCP/IP). The Internet of Things gives everyday devices an IP address and lets them plug into the internet. In 2008, the number of things connected to the Internet was greater than the people living on Earth. Within 2020, the number of things connected to the Internet will be about 50 billion. Therefore, the It will be the most important industrial trend in the next 10 years. Hence the transition from closed networks to corporate networks technology information and public Internet is accelerating at an alarming pace, and justly raising alarms about security [1].

The Internet of things is not consider is a new technology, which emerged in the technology industry, after the computer and the Internet. The internet of things has four main components including information processing ,sensing, applications and services, heterogeneous access, and additional components such as privacy and security [2].

Since become our lives dependent completely on entirely of smart devices and these devices connected to each other via the Internet, hence the privacy has become to the violation and interference of the involved stakeholders. So it is necessary to find a solution to the protection and security [3].

In this paper we will present the security and privacy when using the Internet of Things technology, depending on the architecture of the devices, and will be focusing on how security building in the devices, and protection requirements, by studying the architecture layer and IoT security infrastructure.

The rest of the paper is organized as follows. Section 2, review the security in devices. Section 3, gives an architecture and requirements of IOT security that is present the each architecture layers. Section 4, present security risks for each layers. Section 5, review of some IoT security issues. Section 6, situation of IoT safety .Section 7, concluded the paper content

2. BUILDING SECURITY IN DEVICES
The Security in devices must be addressed throughout the device lifecycle , from the initial design to the operational environment[4]:

2.1 Secure booting
When the device is running for the first time, the authenticity and integrity of the program on the device verification by digital. The same way that the person or to sign a legal document digital signature on the image of the program and check the side of the device ensures only program authorized in that body, which was signed and authorized by the entity will be loaded [5].

2.2 Access control
There are different forms of resources and access controls are applied. Controls in mandatory or role-based access to the built-in the operating system limit the privileges of device components and applications so that they only access to the resources they need to do their job. In the event that any component and access control ensures that, the intruder has minimal access to other parts of the system as possible. Access control list on the device mechanisms are similar to network-based access. Even if someone was able to steal credentials for companies to gain access to network information for the risk of only those areas will be restricted from network authorized by the specific documentation mandate[4].

2.3 Device authentication
When the device is connected to the network, it should authenticate itself before receiving or sending data. Inherent in the devices often do not users have sitting behind keyboards, waiting to input the required credentials to gain access to the network. How, then, can ensure that correctly identify those devices before? As user authentication allows the user to access the corporate network based on password and user name, and authentication device is a device that allows access to the network based on a similar set of credentials stored in a safe storage area [6].

2.4 Firewalling and IPS
The device needs the firewall packet inspection or a profound ability to control the traffic that is destined to end in the device. Why is the wall or host-based IPS protection is

required if the existing devices on the network in place? Inherent devices have unique protocols of its kind, distinct from the company's information technology protocols. For example, smart power grid has its own set of protocols that govern how devices talk to each other. This is why there is a need for industry-specific protocol and deep inspection capabilities to identify malicious payloads hiding in non-US IT protocols need a box filter. The device is not interested in a higher level of filtering, traffic on the Internet common network devices should take care of that, but they do not require specific data addressed to finish on this device in a way makes the best use of the limited available resources computer filtering [6] [7].

2.5 Updates and patches

When switch on the device , the device starts to receive the update of the applications installed in the device, therefore the operators put patches on the devices , then the device need to the authenticate them in a professional manner, not consume bandwidth or affected the technical safety of the devices. Such as Microsoft corporation ,to do update for Windows operating system to its users in a period of time not exceeding 15 minutes, so thousands of devices improves the performance of the operating system basic functions and check for correct of the protection devices and operating systems weaknesses. Corrections must be submitted and software updates a way that maintains a limited bandwidth and intermittent explosive contact integral to eliminate the possibility of compromising the integrity of work completely[4].

3. ARCHETECTURE AND REQUIREMENTS OF IOT SECURITY

If we look at the IoT infrastructure, notice that network layer facing the greatest security challenges. Moreover, have several properties. Requirements security of sensor storage, processing and transmitting information and prevents unauthorized accessing even illegal operation, called confidentiality. Asked to each node which participates in The business services process consider is one of the most important sectors that must be secured and ensure that no tampering of the information contained and outgoing ones , there are some security requirement described as follows [8]:

- Failure tolerance: The system must find alternative node, when occur failure in one of the node, to avoid failure.
- Authentication: Must be authenticating the object and information source.
- Control of Access: The providers of information must be able to implement control of access on the data provided.
- Privacy: Taken that only the information provider is able to infer from observing the use of the lookup system related to a specific customer.

Addition, there are another security requirements for IoT , Which must be taken into account when implementation of IoT such as , user identification , secure storage , identity management, secure data communication, availability , secure network access, secure content, secure execution environment ,tamper resistance.

The IOT security architecture is divided into four levels, Figure [1] illustrates for that [2].

3.1 Physical Layer

In this layer, the data and information collected through peripheral devices (physical equipment), and identifies the physical world, information includes properties of the object, etc. environmental conditions; It includes physical RFID reader equipment and all kinds of sensors Global Positioning System (GPS) and other equipment. The main element of this layer is sensors to capture and represent the material world in the digital world. Because the storage nodes is very short and the power capacity is too, then unable to apply public key encryption algorithm to security protection. In addition, it is very difficult to set up security protection system. Hence, they vulnerable to attacks from the external network such as deny of service also bring new security problems. In the other hand sensor data still need the protection for confidentiality, integrity and authenticity[2].

Firstly, authentication of node is necessary to prevent unauthorized access of node; and secondly to protect the confidentiality of information between a transmitter, the absolute necessity of data encryption, before the data encryption key agreement in advance an important process; It is the strongest safety measures, increased consumption of resources to solve this problem encryption technology become an important weight includes lightweight encryption protocol encryption algorithm. At the same time the safety and health of the sensor data has become the subject of search [9].

3.2 Network layer

The network layer is responsible for the transfer of reliable information from the conceptual layer preliminary information processing and classification through polymerization. In this layer of information transfer depends on several Internet backbone networks, a mobile communications network and satellite television networks and infrastructure wireless network, and communication protocols are necessary also exchange information between devices. In spite of the relatively basic to protect the safety of the network, but the Man-In-the-Middle-Attack attack counterfeit still exist, and at the same time, junk mail, a computer virus cannot be ignored, a large number of transmitted data causes the busiest. Thus the security at this level is very important for the IoT[2].

In this layer, security mechanisms of communication are difficult to implement. Identity authentication mechanism to prevent the contract, out of verse security and confidentiality, and the complementary equally important, we also need to establish a mechanism confidentiality, integrity of data. In addition to distributed denial of service attack, a common attack in the network, particularly in the internet of things even to prevent DDOS attack for the vulnerable node is consider another problem should be solved in this layer [10].

3.3 Support layer

Will be prepared to support a reliable platform to support the application layer, on this platform to support every kind of smart computing power will be organized by the network grid and cloud computing. It plays the role of the combined application of top layer and the network layer to the bottom[2]. The mass data processing to do an intelligent decision for network behavior in support layer, intelligent processing limited to harmful information, so it considered a one a challenge to improve the ability to identify harmful information [11].This layer needs to many of application security structure such as secure multi-party computation and cloud computing, almost all strong encryption algorithms and

protocol of encryption, stronger security system and anti-virus technology [12].

3.4 Application layer

The application layer is the top-level terminal and the station. This Layer provides personal services according to the user's needs. Users can login to the Internet of things through the application interface layer of the mobile PC, TV or equipment and so on. Safety requirements vary on the environment the level of different applications in this layer, and sharing of data is that one of the feature of application layer, which create data privacy problems, information disclosure and access control. We need two aspects to solve the problem of security in this layer. The first is key agreement and the authentication across the heterogeneous network, the second is protection of the user's privacy [2].

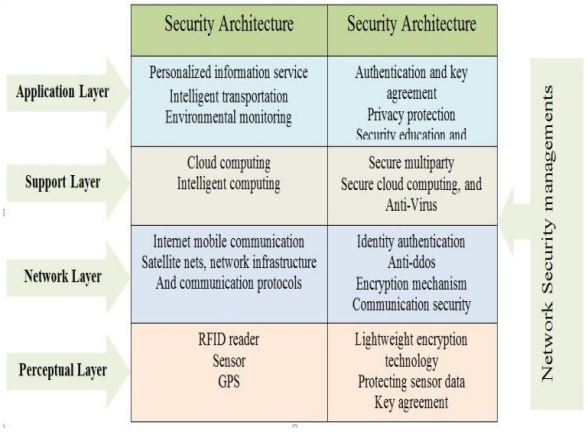

Fig.1 Architecture and Requirements of IOT

4. SECURITY RISKS IN IOT

According to the IoT infrastructure, the IoT is divided into three layers [13]:

- **Perception Layers**: This layer is consider of perceiving and gathering information from the surrounding environment, the attackers can easily eavesdrop the communication link, then they can analyze the data and the role of the nodes to capture the users' information.
- **Network Layer** : This layer is consider of communication or transport layer , the huge amount of data exchange by this layer , which will causes network congestion in the process of transmission . In addition, this is likely to generate denial of service attacks.
- Application Layer: Provide the services for all industries [14], and in this layer the user can get some important real-time information, which is the goal of developing IoT. In some of a specific industry, the application process, layer of perceptive collects huge amounts of data of users, including privacy data. Hence, must protect privacy and individual information .especially the enterprises data.

In the [13] , propose some ways of security, to resolve protection of information privacy , they add third party sever as IoT middleware , and mechanism of encryption/decryption ,furthermore access control. That is consider of improved IoT model for the original infrastructure of IoT Figure [2].

This can effectively prevent the data leaking out in the process of transmission. Moreover, use the third party server to filter before the data access to application layer to ensure the sensitive data did not be stolen or interpolated. Further uses the anonymous processing; only legitimate users passed the authorization can see this processed information. Thus, some users cannot see the privacy data after anonymous processing.

5. SECURITY IOT ISSUES

Wireless sensors network are considered the backbone of the Internet of Things (IoT), WSN's characteristics face some challenges including information security. Physical attacks by attackers, Trojan attacks, virus damage, keys decryption, DOS, eavesdropping and traffic analysis are really threats. The trouble challenge is a key distribution, encryption and decryption mechanism caused by wireless sensor networks large and resource constraints [15] [16]. There are some security's issues, including:

- **Encryption gateway node:** In this way, integrate and combine communication node with key, that is mean encryption node (like sensor node), the attacker hard to be controlled because his need master key of the node. Hence, the find the key is very hard, and he cannot control gateway node and get all information through it. Then he cannot tamper with the sending information.
- **Enhance the capacity against DOS attack: The WSN** must connect to the external network, which including internet, therefore, under attack from other networks, the other may be DOS attack. Since sensors network with a very limited capacity for storage and processing, so the capacity against DOS attacks is weak.
- **The encryption mechanism:** The encryption occurs in the application layer (end to end), and in the network layer (by-hop). By-hop encryption, it provides the protection to links, which asked necessary. But, because the by-hop encryption requires decryption in the transmission nodes, so every node is likely to interpret the clear text message. End to end encryption cannot protect the destination address. This makes encryption not hide the message's source and destination, which is easy, attacked by malicious access cause by analysis of the communication services. Therefor the end-to-end encryption mechanism is still the first choice.

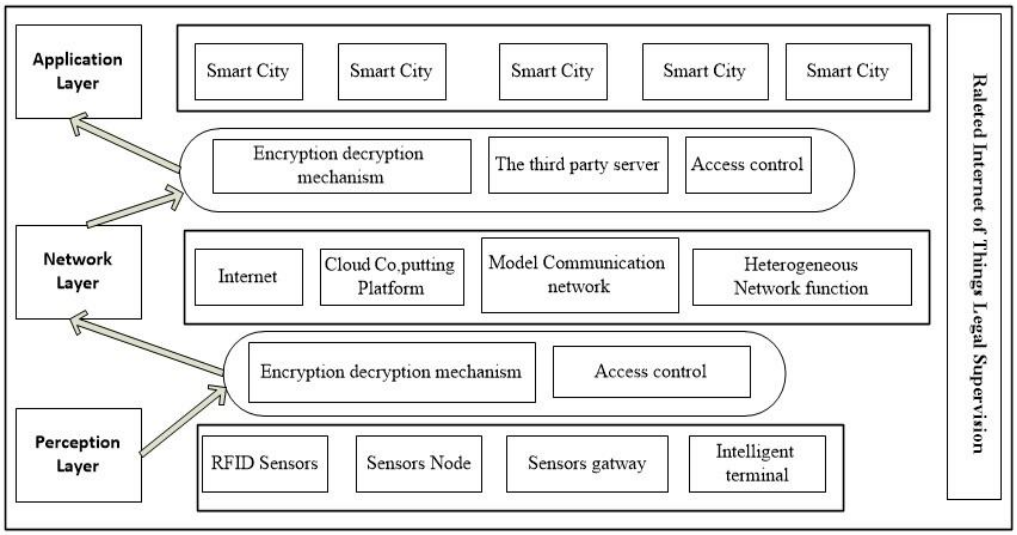

Fig.2 IoT security infrastructure Multi-layer

- **Business authentication:** The business services are very sensitive, it depends on to network layer authentication is responsible for the network identification. Therefore, the network layer authentication is essential, but the application layer authentication is not necessary. In other side if the business is very sensitive such as financial services, the service provider do not trust the security of network , but choose security protection is higher level, it is the time need to be done in the business layer certification.

6. IOT SAFETY SITUATION

The Internet of Things (IoT) is an emerging technology (Hot things), so people focus and attention to this technology, and the result is a lot of security flaws, so the developers intensive attention to the safety of IOT [17].

Safety IoT can divide into perception layer security, network layer security and the application layer security, according to the system architecture. And ensure the IOT safety, on the networking strategy implementation, there are several considerations as following [18]:

- Create safe network environment,
- Use the strong security mechanism to secure the information during of sending.
- Always update the information security protection to increase prevention.
- Make sure to the permission and authentication for the logging network

7. CONCLUSIONS

The Internet of Things, also called The Internet of Objects, refers to a wireless network between objects; usually the network will be wireless and self-configuring, such as household appliances. Secures IOT end-to-end, which means authenticating device communications, protecting code and applications, and securing devices from threats. The architecture and building of things (objects) play an important role in the security of things, when they connect to the general network , and mean of structure of things is the programming architecture, which is responsible for how and way of dealing with the others things around it. In this paper presented the security and privacy when using the Internet of Things technology, depending on the architecture of the devices, and will be focusing on how security building in the devices, and protection requirements, by studying the architecture layer and IoT security infrastructure.

8. REFERENCES

[1] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," Internet of Things Journal, IEEE, vol. 1, pp. 22-32, 2014.

[2] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, 2012, pp. 648-651.

[3] R. H. Weber, "Internet of things: Privacy issues revisited," Computer Law & Security Review, vol. 31, pp. 618-627, 2015.

[4] A. Shipley, "Security in the internet of things, lessons from the past for the connected future," Security Solutions, Wind River, White Paper, 2013.

[5] 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, pp. 3594-3608, 2012.

[6] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer Networks, vol. 54, pp. 2787-2805, 2010.

[7] A. J. Jara, M. A. Zamora, and A. F. Skarmeta, "An internet of things---based personal device for diabetes therapy management in ambient assisted living (AAL)," Personal and Ubiquitous Computing, vol. 15, pp. 431-440, 2011.

[8] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, "Proposed security model and threat taxonomy for the internet of things (IoT)," in Recent Trends in Network Security and Applications, ed: Springer, 2010, pp. 420-429.

[9] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, I. S. Jubert, M. Mazura, M. Harrison, and M. Eisenhauer, "Internet of things strategic

research roadmap," O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, et al., Internet of Things: Global Technological and Societal Trends, vol. 1, pp. 9-52, 2011.

[10] L. Tan and N. Wang, "Future internet: The internet of things," in Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on, 2010, pp. V5-376-V5-380.

[11] D. Uckelmann, M. Harrison, and F. Michahelles, Architecting the internet of things: Springer Science & Business Media, 2011.

[12] L. Da Xu, W. He, and S. Li, "Internet of Things in industries: A survey," Industrial Informatics, IEEE Transactions on, vol. 10, pp. 2233-2243, 2014.

[13] X. Yang, Z. Li, Z. Geng, and H. Zhang, "A multi-layer security model for internet of things," in Internet of Things, ed: Springer, 2012, pp. 388-393.

[14] G. Gang, L. Zeyong, and J. Jun, "Internet of things security analysis," in Internet Technology and Applications (iTAP), 2011 International Conference on, 2011, pp. 1-4.

[15] S. Sharma, A. Sahu, A. Verma, and N. Shukla, "Wireless sensor network security," in Advances in Computer Science and Information Technology. Computer Science and Information Technology, ed: Springer, 2012, pp. 317-326.

[16] C. M. Medaglia and A. Serbanati, "An overview of privacy and security issues in the internet of things," in The Internet of Things, ed: Springer, 2010, pp. 389-395.

[17] S. Peng and H. Shen, "Security Technology Analysis of IOT," in Internet of Things, ed: Springer, 2012, pp. 401-408.

[18] I. Gudymenko and M. Hutter, "Security in the Internet of Things," Proceedings of Intensive Program on Information Communication Security (IPICS 2011), pp. 22-31, 2011.