Internet of Things: Architecture, Security challenges and Solutions

Siham Al Hinai[1], Ajay Vikram Singh[2]

[1,2]*Middle East College, Muscat, Sultanate of Oman*
salhinai@mec.edu.om, asingh@mec.edu.om

Abstract: ***Internet of things (IoT) is a large distributed network in which billion of devices are interconnected. It is considered to be the largest wave of resolution as it does not require human to machine interaction. However, with the rapid growth of IoT, challenges in terms of security have evolved as well. Since IoT consists of three layers perception layer, network layer and application layer, this paper will provide an analysis for various security problems at each layer including the cross-layer heterogeneous integration security issues and suggest some promising solutions.***

Keywords: IoT, DOS, Wi-Fi, RFID, and NFC

I. INTRODUCTION

Internet of Things (IOT) is playing a crucial role after its appearance. It is covering a verity range of devices starting with the traditional ones up to the household objects such as WSNs and RFID. It is expected to be the upcoming generation of the internet in which billion of things are interconnected [12]. It allows machine to machine (M2M) communication where larger "things" will be able to communicate through the wire lines such as fiber optic and Ethernet. Furthermore, most of the connections are expected to take place via wireless networks with mini chips embedded into the "things" using various standards such as ZigBee, Wi-Fi, Bluetooth, RFID, and NFC in order to achieve an effective communication [1][6].

It is leading to more "connected life" through connecting everyday items such as household appliances, smart phones, watches and wearable fitness devices to networked devices such as laptops, computers, and smartphones, allowing them to communicate and transfer data among each other [2].

There are two categories for the challenges faced by IoT; Security and Technological challenges. Security challenges are related with authentication, confidentiality and integrity of the data transferred through IoT. While Technological challenges are more related with the energy and scalability resulted from the dynamic nature of IoT devices.

IOT has three layers architecture, (Perception layer), where the sensing devices are unable to provide a proper level of protection due to their energy limitation ;(network layer), IoT relies on networking and communication to facilitate the transaction process. However, it is prone to eavesdropping, interception and DOS attacks; and (application layer) a user interface which needs data aggregation and encryption which to handle vulnerability and scalability problems of all layers. Other than the issues found in each layer, cross layer heterogeneous integration have some security issues which need to be solved [3].

Since IoT is a new technology, it is expected that it will phase lot of challenges and concerns. In different sections of this research different security issues and counter measures are discussed. Issues associated with each layer and their counter measures are discussed. In addition the cross-layer heterogeneous integration issues are also analyzed.

II. IOT ARCHITECTURE

The IoT layers differs from each other by the roles they play and the devices operating at them. There are many opinions about the number of layers in IoT [15]. However, most of the research papers emphasized three main layers in IoT. Figure 1 illustrates the IoT architecture which consists of three layers [7].

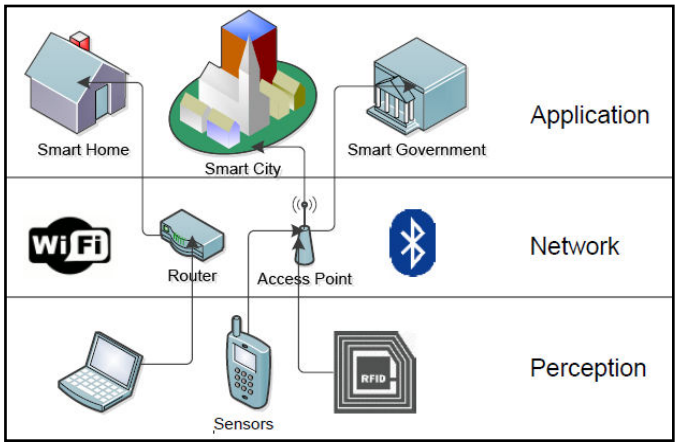

Fig. 1. A generic service-oriented architecture for IoT

Perception layer is concerned with collecting and sensing the information of IoT objects. The collection of information is done in this layer with the help of different devices such as sensor nodes, smart cards and RFID tags.There are two major component or sub part of this layer: Perception node and

978-1-5386-0514-1/17/$31.00 ©2017 IEEE

perception network [4]. Perception node such as controllers or sensors are used for data control and data acquisition. While perception network is used to send control signals to the controller or send the collected data to the gateway to be transmitted in the Network Layer.

Network layer has the function of managing wireless and wired connections. It transfers the gathered data through the sensors, and computers across the wired and wireless networks .It can also support connection oriented service through maintaining reliability of data delivery. Routing takes place at this layer where data is transmitted across different IoT devices and hubs over the internet. Routing, switching, gateway devices operates at this layer using variety of technologies such as Zigbee, WiFi, 3G, Bluetooth and LTE [5][10]. The gateway acts as a medium between separate IoT devices by aggregating, filtering and moving data between different sensors.

Application layer is the interface between the applications and the end users. It provides the means for the communication between them. It can support various services required by business. In addition, it recognizes the resource allocation and computation in producing, processing, screening and selection of data. It has the ability of recognizing spam data, malicious data and valid data through its filtering feature [9].It resolves the received information and make control decisions to allow the achievement of intelligent processing by identification, connection, and control between devices and objects. It is also known as Process layer.

III. SECURITY CHALLENGES AND COUNTERMEASURES IN EACH LAYER

Each IoT layer is prone to security attacks and threats which can be either passive or active. Passive attack monitors the IOT network data without affecting or interrupting the services. While an active attack completely stops the services causing drawback in the network performance. Moreover, all layers are susceptible to one common attack which Denial of Service attacks (DoS), which can prevent an authorized user form utilizing the network resources, devices and services. Below is a comprehensive analysis of security problems faced at each IoT layer [13].

Perception Layer-The IoT perception layer is facing three security issues. First, IoT nodes operate in outdoor environment, leading to physical attack where the hardware components can be tampered by the attacker. Second, the heterogonous nature of the dynamic network allows mobility of IoT devices. However, due to the computation capability, power consumption, and storage capacity limitation, it makes them susceptible to many kinds of threats and attacks. Third, since IoT uses wireless technologies for transmission of information, other existing waves can cause reduction in the strength of the wireless signals. Different types of attacks can exploit the confidentiality of this layer[11].

For example, Replay Attack which is caused by replaying or alerting or spoofing the identity information of an IoT device. In addition, the attacker could analyze the required time needed to perform the encryption in order to gain the encryption key which is identified as Timing Attack. Another possible attack targeting confidentiality is Node Capture attack, where the attacker takes over the node and captures all data and information. Also, the attacker might add another node in the network which sends malicious data affecting the data integrity.

DOS attack can also arise through the consumption of nodes energy by preventing them from going into sleeping mode during times of less demand. The above mentioned problems of the Preception layer can be overcomed by the use encryption which is the study of cryptography and authentication which is used to identify the users prior communication. The following is a table of security concerns at Perception layer.

TABLE 1: Security Concerns at Perception layer

Security threats	Description
Unauthorized access	Due to physically capture or logic attacked, the sensitive information at the end-nodes is captured by the attacker;
Availability	The end-node stops to work since physically captured or attacked logically;
Spoofing attack	With malware node, the attacker successfully masquerades as IoT end-device, end-node, or end-gateway by falsifying data
Selfish threat	Some IoT end-nodes stop working to save resources or bandwidth to cause the failure of network
Malicious code	Virus, Trojan, and junk message that can cause software failure
Denial of Services (DoS)	An attempt to make a IoT end-node resource unavailable to its users
Transmission threats	Threats in transmission, such as interrupting, blocking, data manipulation, forgery, etc.
Routing attack	Attacks on a routing path

Network Layer- As mentioned before, the transmission medium's broadcast nature and the sensor node's computation and power limitation makes network layer more prone to DOS attacks. Aside from the DoS attacks, the privacy and confidentiality of the network layer can be compromised by passive monitoring, traffic analysis and eavesdropping attacks. These attacks occur due to the data exchange between the devices and remote access mechanisms which are the main functions provided by this layer.

Since this layer can experience an eavesdropping, it is therefore more likely to suffer from Man in the Middle Attack. Securing Key exchange process can prevent an attacker from eavesdropping the keying material and performing an identity theft. In addition, due to the heterogeneous nature of IoT, the current utilized network protocols might not be sufficient and needs to be upgraded. Although IoT provides the ability of automatic data transfer across the network without requiring human to computer or human to human interaction by introducing machine-to-machine communication, attackers can make use of all devices and objects which are connected to perform information theft and criminal activities. Therefore,

protecting the objects is equally important to protecting the network. Objects should have a mechanism for sensing network threats and providing the necessary protection against various network attacks. This can be accomplished by designing software and protocols which can allow device instant reaction against unexpected situation which can have a negative impact on the security.

In addition, encryption mechanisms, authentication, key management and secured routing protocols can be used. However, due to the resource limitation, just light weight algorithms can be used to find balance between security and power consumption. The following are the security concerns at the Network Layer.

TABLE 2: Security Concerns at Network layer

Security threats	Description
Data breach	Information release of secure information to an untrusted environment
Transmission threats	The integrity and confidentiality of signaling,
Denial of Services (DoS)	An attempt to make a IoT end-node resource unavailable to its users
Public key and private key	The comprise of keys in networks
Malicious code	Virus, Trojan, and junk message that can cause software failure
Transmission threats	Threats in transmission, such as interrupting, blocking, data manipulation, forgery, etc.
Routing attack	Attacks on a routing path

Application Layer- The application layer has many security related issues as IoT lacks standards and global polices that controls the development and the interaction between different applications [14]. The different utilized authentication mechanisms by the applications makes the integration among them difficult while simultaneously ensuring identity authentication and data privacy. The big amount of data that is shared by the connected devices can result into a large overhead on the applications that analyze the data leading to a great impact on the services' availability. There are several things to keep in mind when designing an applications in IoT, the amount of data that will be shared, the interaction nature between various users and different applications, and the application management. Some tools must be designed to allow the users to have control upon data disclosure and authenticate the other communication parties. The following are the security concerns at Application Layer [8].

TABLE 3: Security Concerns at the Application layer

Security threats	Description
Remote configuration	Fail to configure at interfaces
Misconfiguration	Mis-configuration at remote IoT end-node, end-device, or end-gateway
Security management	Log and Keys leakage
Management system	Failure of management system

IV. CROSS-LAYER HETEROGENEOUS INTEGRATION ISSUES

The three layers of IoT architecture exchange the information between them to achieve the interoperability between devices and services. Therefore, some of challenges for security occur are privacy for the users and associated data, securing the shared data across the layers, and trust guarantee among the communication parties. These challenges are predicted as IoT connects different units with different venders, complexity and capabilities. It provides connections between heterogeneous networks and things. In addition, IoT supports dynamic environment where devices can rapidly change their connections to be with other set of devices. Therefore, all the three layers of IoT requires security measures; at Perception layer for data acquisition and, at network layer for data transmission, at application layer to manage data's integrity, confidentiality, and authentication[5].

V. CONCLUSIONS

The security issues at IoT architecture was the focal point of this paper. Services provided by each layer have been highlighted as well as the security issues were introduced. In addition, the security challenges across the layers have been analyzed .It was observed that each layer from the IoT framework is exposed to different types of attacks. For this reason, many security challenges need to be solved. IoT is an innovative technology but still in its early development stage. There are some further studies which research can focus on such as developing lightweight cryptographic algorithms, and developing a secured architecture for IoT system.

REFRENCES

[1] Britton, K., 2016. Handling Privacy and Security in the Internet of Things. *Journal of Internet Law,* p. 6.

[2] Li, B. & Li, Y., 2017. INTERNET OF THINGS DRIVES SUPPLY CHAIN INNOVATION. *international Journal of Organizational Innovation,* p. 23.

[3] Mayuri, A. B. & Sudhir, T. B., 2015. Internet of Things: Architecture, Security Issues and Countermeasures. *International Journal of Computer Applications (0975 – 8887),* p. 4.

[4] Qi, J. et al., 2014. The Internet of Things: A Security Point of View. *Springer Science,* p. 21.

[5] Tasneem, Y., Rwan, M., Fadi, A. & Imran, Z., 2015. Internet of Things (IoT) Security: Current Status, Challenges and Countermeasures. *International Journal for Information Security Research (IJISR),* p. 9.

[6] Atzori, L., Iera, A., Morabito, G., and Nitti, M. (2012), "The Social Internet of Things (Siot)–When Social Networks Meet the Internet of Things: Concept, Architecture and Network Characterization, " *Computer Networks*, Vol. 56, No. 16, pp. 3594-3608.

[7] Bamforth, R. (2014), "Internet of Things, Scada, Ipv6 and Social Networking," http: //www.it-director.com/business/innovation/content.php?cid=14590, Retrieved 14th December 2013.

[8] Bi, Z., Xu, L., and Wang, C. (2014), "Internet of Things for Enterprise Systems of Modern Manufacturing, " *Industrial Informatics, IEEE Transactions on*, Vol. 10, No. 2, pp. 1537 - 1546.

[9] Cai, H., Xu, L., Xu, B., Xie, C., Qin, S., and Jiang, L. (2014), "Iot-Based Configurable Information Service Platform for Product Lifecycle Management, " *Industrial Informatics, IEEE Transactions on*, Vol. 10, No. 2, pp. 1558-1567.

[10] Chen, Y., Han, F., Yang, Y.-H., Ma, H., Han, Y., Jiang, C., Lai, H.-Q., Claffey, D., Safar, Z., and Liu, K.R. (2014), "Time-Reversal Wireless Paradigm for Green Internet of Things: An Overview, " *Internet of Things Journal, IEEE*, Vol. 1, No. 1, pp. 81-98.

[11] Choi, J., Li, S., Wang, X., and Ha, J. (2012), "A General Distributed Consensus Algorithm for Wireless Sensor Networks, " *Wireless Advanced (WiAd), 2012*, London, United Kingdom: IEEE, pp. 16-21.

[12] Council, N. (2008), "Disruptive Civil Technologies: Six Technologies with Potential Impacts on Us Interests out to 2025, " *Conference Report CR*.

[13] Ajay Vikram Singh, Bani Singh, M. Afshar Alam, “Issues and Challenges associated with Secure QoS aware Routing in MANETs” , International Journal of Research and Reviews in Ad Hoc Networks (IJRRAN), Vol. 1, No. 3, pp. 73-76,ISSN: 2046-5106, Science Academy Publisher, United Kingdom, September 2011.

[14] Ajay Vikram Singh, Vandana Juyal, Ravi Saggar, “Trust based Intelligent Routing Algorithm for Delay Tolerant Network using Artificial Neural Network”, Wireless Networks (WINE), Springer Publication, US, Volume-22, Issue-135 pp 1-10.

[15] Fielding, R.T., and Taylor, R.N. (2002), "Principled Design of the Modern Web Architecture, " *ACM Transactions on Internet Technology (TOIT)*, Vol. 2, No. 2, pp. 115-150.