Security Building Blocks in Internet of Things (IoT) for Providing Adaptive Mobile Web Services

Feda AlShahwan
College of Technological Studies
Public Authority for Applied Education and Training
P.O. Box 23167, Safat 13092, Kuwait
Phone: 965 1 806611
fa.alshahwan@paaet.edu.kw

Maha H. Faisal
Kuwait University, Computer Engineering Department
Jamal Abdul Nasser St, Kuwait
Phone: 965 2498 8888
maha.faisal@ku.edu.kw

Abstract

A radical evolution of the current Internet into a Network of interconnected objects that not only senses information from the environment and interacts with the physical world, but also uses existing Internet standards to provide services for information transfer, analytics, applications and communications results in an enormous amount of vital applications. The pervasive nature of the information sources means that a great amount of data pertaining to possibly every aspect of human activity, both public and private, will be produced, transmitted, collected, stored and processed. Consequently, integrity and confidentiality of transmitted data, as well as the authentication of (and trust in) the services that offer the data, is crucial. Hence, security is a critical functionality for the ***Internet of Things*** (IoT). The enormous growth of mobile devices capability, critical automation industry fields and the widespread of wireless communication cast need for the seamless provision of mobile web services IoT environment. These are enriched by mobile cloud computing. However, it puts a challenge to its reliability, data authentication, power consumption and security issues. There is also need for auto- self-operated sensors for geo-sensing, agriculture, automatic cars, factories, roads, medicals application and more. IoT is still highly not reliable in points of integration between how its devices are connected; this means that there is poor utilization of the existing IP security protocols.

Our solution is based on the use of existing security protocols between clients and the mobile hosts as well as a key management protocol between the individual mobile hosts implementing an out-of-band key exchange that is simple in practice, flexible and secure. We study the performance of this approach by evaluating a prototype implementation of our security framework. This paper at a preliminary manner, discusses the threats, hacks, misguided packets, over read sensor message. These packets are then translated by hardware and pushed through the web for a later on action or support. Our testing to a set of sensor triggered scenario and set up clearly indicates the security threats from a wireless connected small LAN environments and the overestimated sensor messages resulting from the initial set of the sensor readings, while we emphasize more on the security level of the web services serving the IoT connected device.

Keywords: Internet of Things; Network of Things; Wireless sensor Networks.

1. Introduction

In the past decade, a lot of research has been done into the investigation of ***Internet of Things*** IoT (Woo & Culler, 2001). The system which includes devices that are connected over the internet and communicate directly with each other is called IoT. In this paper, we propose a deep penetration method for the IoT connected set of devices, along with the mobile cloud. Architecture and testing framework for providing mobile cloud computing in the IoT, that is based on the object security, power utilization, latency measures, and packet loss rate are explained.

Internet protocols were introduced as safe and secure data packets. These are the solid protocol to capture the packets within the services provided and served by the internet, as a ***World Wide Web*** (WWW), as ***Fiber to the Premises*** (FTTP), Mail, video streaming and serving other protocols, presenting an edge to the web. In the last decade, a new era of security was introduced while testing and applying the new sensors and web service to the scene of internet as more and more automation was introduced and tested for manufacturing purposes, statistics, traffic jam monitoring, file processing within factories, energy saving techniques, medical sensitive data and alert applications.

An alert application includes measuring on a remote site, the systolic and diastolic pressure, patient's heart rate, pulse of a patient and sending out the sugar glucose far from the hospital. In addition to this, testing results from a patient’s home, while he or she performs the test. A smartphone scans and senses the result and sends it via the web (an internet protocol), through a smartphone application.

While using a wireless network, WiMAX, 3G, LTE, or 4th generation communication protocol, networks or simply a fixed network such as ***Asymmetric Digital Subscriber Line*** (ADSL) services (medium) known as in industrial services. For example, an immediate auto shut off power is required for an overheated oven in an electric factory or an overcrowded traffic road. This helps to send a report of a series of processed photos to the operation center periodically, which would alert either a police patrol or movement to the site to clear the crowd or to solve the accident caused by traffic jam reasons. The same set of steps are presented to show a critical case or a critical disruption of the normal settled case or the normal routine and this is when an indict application for Internet came to the scene of technical processed signals and connected smart devices.

Internet security is a major research topic in the field of computing and parallel processing, networking and data network design. There are many faces to how such entity or terminology is defined. The term IoT (Atzori, Iera, & Morabito, 2010) mainly refers to internet-connected objects that are smart in a computational and connectivity manner. These objects are able also to compute, detect and communicate while making measurements for various functions. Functions include civil, domestic, manufacturing, industrial applications, automation and medical applications that bring new protocols to life, such as ***Time Division Multiple Access*** (TDMA collision-free protocol), ***Carrier Sense Multiple Access*** (CSMA -slow and low traffic level). These protocols are applied to sensors of the IoT system and form the backbone for the communication of the semsors in IoT system. An energy efficient MAC protocol and appropriate routing protocols are required in the IoT networks with limited resources. Several MAC (Juels, 2012) protocols have been proposed for various domains with TDMA, CSMA and ***Frequency Division Multiple Access*** (FDMA). These protocols are collision-free. However, they require additional complexity to the sensors. Moreover, none of these protocols are accepted as a standard. Therefore, the significance of this scenario requires further research.

The connection is not stable for a number of reasons. For instance, the battery of the sensor may drain out, the wireless communication can be interrupted or a sensor drops out. Consequently, a methodology for self-adapting to the IoT system must be applied that allows for multi-path routing scheme. Multi-path routing protocols are used in mobile ad hoc networks and terrestrial WSNs (Aoudia, Gautier, Magno, Berder, & Benini, 2016; Hasan, Al-Rizzo, & Al-Turjman, 2017). They are mainly divided into three categories namely data-centric, location-based and hierarchical (Bakht & Shaikh, 2016). This classification is based on different application domains. Data-centric protocols are query-based and they depend on the naming of desired data, which helps in eliminating unessential transmissions. Location-based protocols utilize the position information to relay the data to the desired regions rather than the whole network (Amsalu, Zegeye, Hailemariam, & Astatke, 2016). Hierarchical protocols aim at clustering the nodes so that cluster heads can do some aggregation and reduction of data in order to save energy. The main challenge for the existing routing protocols is preserving energy. This is due to the scarcity of resources. Energy in the IoT network will dominate the number of hops in the multi-hop scenario.

IoT has immense potential to change many of our daily activities, routines, and behaviors. Thus the next era in the field of networks will be outside the realm of the traditional static network. In the IoT system, many of the objects that surround us in our daily life, like homes, medical centers, factories, hospitals or government processes areas and universities, will be active via web services. IoT smart items or gadgets are simply an object of the network that can receive, send and translate information through a ***Transmission Control Protocol*** (TCP) or by using sensor elements that can convert their sensors into signals.

The information and communication systems of the IoT networks involve a significant amount of data that have to be stored, processed and interpreted in a seamless, efficient and easily presented form. New sensor network technologies will emerge to meet the enormous amount of data and the new challenges in this system. This model will consist of a session (alert, emails triggers, reports, actions movement, stopping of movement, narrow down, widening etc.) that delivered in a seamless uninterruptible and efficient manner. Cloud computing can provide the virtual infrastructure for such computing model which integrates monitoring devices, storage devices, sensors, etc.

The remainder of this paper is structured as follows; the next section starts with a brief history of the emerging technology of the IoT with its associated applications. This is followed by an introduction of the cloud computing technology and others that have impacts on the IoT. An analysis of the IoT components is presented in section 4.0. A study of some of the technologies that are developed to implement IoT is demonstrated in section 5.0. After that, the challenge issues that cope against the development of the IoT are raised in section 6.0. The solution of the Securities and Threat Taxonomy for IoT is explained in section 7.0.

2. Background and History

IoT requires the usage of the limited network resources. The existing networks and context-aware computation emerge the application of smart connections. The instant presence of the data and the high-speed communication networks are the results of the growing presence of LAN, 3G, WiFi, WiMax, 4G and LTE wireless Internet access. However, for the successful emergence of the IoT vision, the computing system will need to convert from the traditional mobile computing scenarios that use smartphones and wireless network and move into connecting smart objects and embedded intelligent devices. This transition for the IoT demands the following (Botta, De Donato, Persico, & Pescapé, 2016):

- A public or private accessible and shared environment that considers the context of its users and their appliances;
- Software structure and communication networks to process and transfer the relevant data, information to where it is related;
- The analytic tools in the IoT that have the characteristic of automation and adaptive behavior.

Smart connectivity and context-aware computation of the IoT system can be accomplished with the application of these aforementioned fundamentals. IoT is a representation of a ***Network of Things*** (NoT), more clearly, IoT has its own objects that are connected to the Internet, while NoT can be considered as ***Local Area Network*** (LAN), with none of its objects connected to the Internet. Social media networks, sensor networks, are all versions of NoTs.

It is common to call NoT within a work environment as an enterprise based application. The Information that is gathered and processed in these networks is tailored to be used only by the enterprise owners and the data may be revealed selectively (Urzaiz, Hervas, Fontecha, & Bravo, 2016). An example of NoT applications is environmental monitoring, which is implemented to monitor and track the number of facility users and manage the utilities. E.g. controls AC, electricity, Alerts, Heat, ventilation, and power.

The evolution of the current Internet into a network of interconnected objects, or gadgets, not only sense information from the surroundings and interact with physical world but also allow using existing Internet standards to provide services for information transfer, analysis of data and web services .Web services are manipulated by the abundant devices and accessed by the open wireless technology such as Bluetooth, WiFi, ***Global System for Mobile communication*** (GSM), Wi-Max and ***Digital Subscriber Line***(DSL) data access, along with tailored sniffers and sniff blocks(Negi, 2014). Recently, in 2012, the number of interconnected things invaded the lives of a visible number of individuals. As we are working on this paper, there are 9 billion interconnected things and it is expected to reach 20 billion devices by 2020.

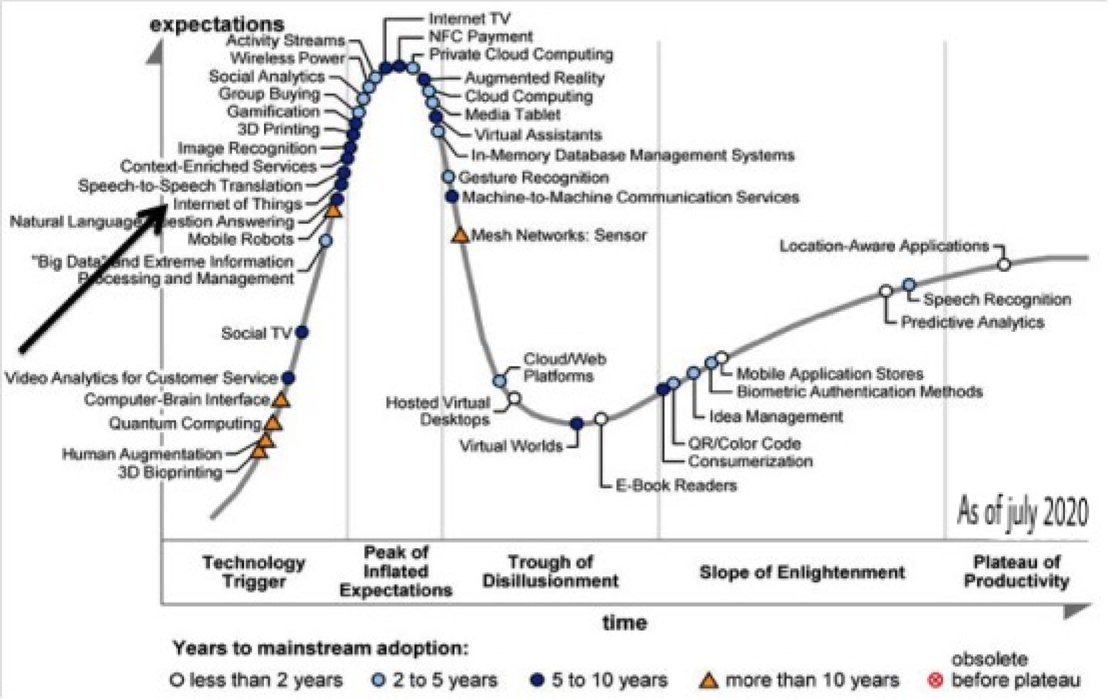

Figure 1. Cycle of technologies during the years

According to the above Gartner's IT Hype Cycle [4] (Figure 1), IoT has been identified as one of the most emerging technologies in IT. A Hype Cycle is a way of representing the emergence, maturity, adoption, and impact on applications of specific technologies ("Hype Cycle "). It is obvious that IoT will take 5–10 years for market adoption. Furthermore, Mobile applications and IoT will be the most disruptive class of technologies over the next 10 years. Gartner explains IoT as a network of physical objects that contains embedded technology to communicate and senses or interacts with its internal states or the external environment. But, for the successful spread of Internet of Things, the computing criterion needs to go beyond traditional mobile computing and evolve into connecting everyday existing objects and embedding intelligence into our environment (Sudarshan, Khan, Dao, & Pham).

Table 1 below describes the smart environment application domain, where smart is a reference to a direct intelligent part or component of the network or IoT.

It explains the type of the network against the criterion. For the smart home, smart retail, network size is expected to be small and the numbers of users are few. While for smart agriculture and smart water the network size needs to be large as the users are not few. The mode of energy in all the application domains is either rechargeable or energy harvesting.

Table 1. Smart environment application Domain

	Smart Home/Office	Smart Retail	Smart City	Smart Agriculture/ Forest	Smart Water	Smart Transportation
Network Size	Small	Small	Medium	Medium/Large	Large	Large
Users	Very few, family members	Few, Community level	Many, policy makers, general public	Few, landowners, policy makers	Few, government	Large, general public
Energy	Rechargeable battery	Rechargeable battery	Rechargeable battery, Energy harvesting	Energy harvesting	Energy harvesting	Rechargeable battery, Energy
Internet connectivity	Wi-Fi, 3G, 4G LTE, backbone	Wi-Fi, 3G, 4G LTE backbone	Wi-Fi, 3G, 4G LTE backbone	Wi-Fi, Satellite communication	Satellite Communication	Wi-Fi, Satellite Communication
Data management	Local server	Local server	Shared server	Local server, Shared server	Shared server	Shared server
IoT Dervices	RFID, WSN	Smart Retail	RFID, WSN	WSN	Single sensors	RFID, WSN, Single sensors
Bandwidth requirement	Small	Small	Large	Medium	Medium	Medium/Large
Example testbeds	Aware Home	SAP future retail center	SmartSantan, CitySense	SisViA	GBROOS, SEMAT	A few implementations

3 IoT and cloud internet in the coming years

Oxford defines the IoT as a proposed development of the Internet in which everyday objects have network connectivity, thus enabling them to send and receive data. The IoT is a term used to describe all connected objects nodes and computers that can and will perform a predefined set and a measurable set or group of functions and actions that send reports which react to a certain probe, indicating a signal as a response a to a unique sensor trigger.

The enormous spreading of smartphones and other handheld devices in the current decade has changed the computing environment. It becomes more autonomous, interactive and informative. Consequently, it motivated the researchers to focus on a human-to-human interface in late 1980. As a result, the Ubiquitous Computing (UbiComp) technology has emerged. Mark Weiser, the forefather of UbiComp, defined a smart environment(Streitz & Markopoulos, 2016) as the physical world that is richly and invisibly interwoven with sensors, actuators, displays, and computational elements, embedded seamlessly in the everyday objects of our lives, and connected through a continuous network.

The creation of the Internet has marked a foremost milestone towards achieving UbiComp‘s vision which enables individual devices to communicate with any other device in the world.

Caceres and Friday (GAO & CHEN) discuss the progress, opportunities, and challenges during the 20 year anniversary of UbiComp. They discuss the building blocks of UbiComp and the characteristics of the system to adapt to the changing world. More importantly, they identify two critical technologies for growing the UbiComp infrastructure *Cloud Computing* and the *IoT*.

The advancements and convergence of micro-electro-mechanical systems (MEMS) technology, wireless communications and digital electronics have resulted in the development of miniature devices having the ability to sense, compute and communicate wirelessly on short distances. These miniature devices called nodes, interconnect to form a ***Wireless Sensor Network*** (WSN) and find wide application in environmental monitoring, infrastructure monitoring, traffic monitoring, retail, etc.(Herr, Kassimis, & Stevens, 2015; Woo & Culler, 2001).

In all of the previous cases, there has to be a governing protocol that authenticates measures and monitors the amount of work needed to perform the pre-described functions, we still have to emphasize the need for new protocols to control and stabilize the IoT environments, such CoCa.

CoCa is an example of a service infrastructure for the IoT that provides pervasive services and supports connecting embedded objects, backend systems, and mobile devices in a seamless manner.

In this paper we shall investigate the security issues and threats that are passed through a uniform and stable environment making use of a pre-set of works, function and signals, reports, etc, working under an IoT rule. More importantly, we shall put and entail the environment to the security text needed to ensure that there is a stable solid system with a model for traffic and car, road monitoring system, enabled with 5 sensors for flow, speed, sudden jam and total size of roads. Here, we use a model for a cloud computing, connected to a .net system named CIT- prepared and authored by Kuwait University undergraduate to manage, and extract useful data and send it over to the control room by making use of its protocols. We shall narrow the testing or hypothesis of this research paper to tackle and modify the working conditions of a Wi-Fi operated medium of an IoT scenario. This paper aims to measure the lack of security and proposes more protocols and shows integration effort to the standards that govern any IoT environment. We propose the paper as a proof that the IoT is not secure enough to withstand critical application, industrial function, and high security. In addition to this, the abundance of Wi-Fi protocols and rules puts the IoT critical applications at risk, but also leaves a lot of questioning on how the procedure or the IoT is designed to operate.

We propose that the IoT is not an optimal secure environment when critical applications are needed, whether in wireless connected machines or wired data networks.

4. Definitions, Terminology, and Elements

As identified by Atzori et. al.(Atzori, et al., 2010), IoT can be realized in three paradigms – internet-oriented (middleware), things oriented (sensors) and semantic-oriented (knowledge). IoT can be more useful in applications where the three paradigms exist.

The RFID group defines IoT as – the worldwide network of interconnected objects uniquely addressable based on standard communication protocols (Gubbi, Buyya, Marusic, & Palaniswami, 2013).

IoT has been defined by a group European research projects as (Tomar, Chaudhari, Bhadoria, & Deka, 2016) things that are active participants in business, information and social processes where they are enabled to interact and communicate among themselves and with the environment by exchanging data and information sensed about the environment, while reacting autonomously to the real/physical world events and influencing it by running processes that trigger actions and create services with or without direct human intervention.

Smart environment (Li, Da Xu, & Zhao, 2015) utilizes information and communications protocols to make the critical medical or emergency, data and health hazard, data structure components, services of a whole town management of traffic or education, healthcare, public health, real estate, and other utilities, more aware, interactive and efficient.

In our view, we make the definition more user oriented and close to real life, as possible, thus generating data objects such as sensors, emails, physical alerts, trigger alarms, messages, emergency warnings, actions etc. without restricting it to any standard communication protocol. This will provide a significant amount of applications. Moreover, it allows using the traditional existing protocols to deploy long-lasting applications on the fly and at any time. Thus, our definition of IoT for smart environments is the communication of sensors and actuating devices to provide information across different platforms that can be accessed through a unified infrastructure, developing and enabling innovative applications. This is achieved by seamless large-scale sensing, data analytics and smart information interpretation using UbiComp and cloud computing.

The components for IoT can be classified from high-level perspective into three categories that enable seamless UbiComp. Each category can be classified into more taxonomies as found in (Atzori, et al., 2010; Crooks, Schechtner, Dey, & Hudson-Smith, 2017; Streitz & Markopoulos, 2016). The three IoT components are:

a) Hardware: made up of sensors, actuators and embedded communication hardware
b) Middleware : on-demand storage and computing tools for data analytics
c) Presentation: novel easy to understand visualization and interpretation tools which can be widely accessed on different platforms and which can be designed for different applications.

The major properties that compose or make the security issues of IoT and also ask for more security reliable measure for IoT, as listed below:

1- Embedded utilization

Most IoT devices have only one single function or use (such as trigger light, turn on power, emerge alerts, message, control, sending data monotone house appliance etc.), as a direct result the recognition to a unique device makes up a pattern that gives an easy profile or can be filtered into a pattern.

2- Divers

The device of IoT is able to work across multiple spanned devices of computing from low-end and low-frequency RFID to full function computers, thus the privacy policy must encompass all the range of computations;

3- Scale

These devices, IoT functional ones are easy to use and are added into the market with simply, easy to use applications, thus it makes it hard for users to monitor the privacy and security issues at a question,

4- Mobile

Most if not all IoT devices are mobile and usually connected to the internet via a large multiple set of services or service providers

5- Wireless

IoT devices, in most cases, get connected, and are thus enabled and become functional to the internet via a large list of wireless protocol namely Wi-Fi, 802.11 ,WiMax, GSM, Bluetooth etc.

5. IoT Supported Technologies

Since these applications were very useful, new technologies have been developed to implement WSN applications. Some of the standard based protocol stacks include 6LoWPAN, IEEE802.15.4e (Shahid, Simon, Joel, Utz, & Thiemo, 2014), ***Routing Protocol*** (RPL) and ***Constrained Application Protocol*** (CoAP) for the management of layer-related procedures.

6LoWPAN is the first wireless connectivity standard that was created for the IoT (Hara et al., 2005). 6LoWPAN standard is defined by IETF to transmit IPv6 packets through computationally constraint networks

RPL stands for Routing Protocol for low power and lossy network. It can support a wide variety of different link layers, including ones that are constrained, or typically utilized in conjunction with host or router devices with very limited resources. Also, it can build up network routes, to distribute routing knowledge among nodes and to adapt the topology in a very efficient way.

Constrained Application Protocol (CoAP) is a software protocol intended to be used in very simple electronic devices that allows them to communicate interactively over the Internet. CoAP is designed to easily translate to HTTP for simplified integration with the web, while also meeting specialized requirements such as multicast support, very low overhead, and simplicity. Multicast, low overhead, and simplicity are extremely important for Internet of Things (IoT). CoAP can run on most devices that support UDP or a UDP analogue. Californium (Cf), Erbium (Er), and Copper (Cu) (Bormann, Castellani, & Shelby, 2012). are three implementations of CoAP. CoAP/UDP works well with IEEE802.15.4 since the MTU (Maximum Transmission Unit) is small. However, in a MAC with larger MTU at high rates, like WiFI IEEE802.11 family, with a MTU of 1500 Bytes, a HTTP transactions can be done with one packet at larger distances. CoAP uses the REST architectural style. A comparison between CoAP and HTTP has taken place in (AlShahwan & Faisal, 2016) to measure their transmission delays and response time. A critical analysis of CoAP and Http is carried out experimentally. The results of testing suggest that CoAP protocol works better in transferring small transaction.

A set of pervasive computing devices that monitors the technology applied to IoT is a characteristic that creates a set of challenges that need to be tackled. The challenges are listed in the following section:

6. Challenges and issues in IoT

There are some issues that act as a barrier against the spreading of IoT:

1. Heterogeneity of devices and its management;
2. Privacy and security of the data packets moved (transported) across these devices, thus a certain level of reliability must be built;
3. Network knowledge and content of the packets need to be known, measured and identified.

The challenges will directly dictate a development of new algorithms that are encrypted in an efficient way to provide a minimum level of security for IoT connected devices and its environment, namely a need for a confidential and highly integral level of data communicating across such service level connected devices.

The following figure illustrates how to provide the level of security for IoT:

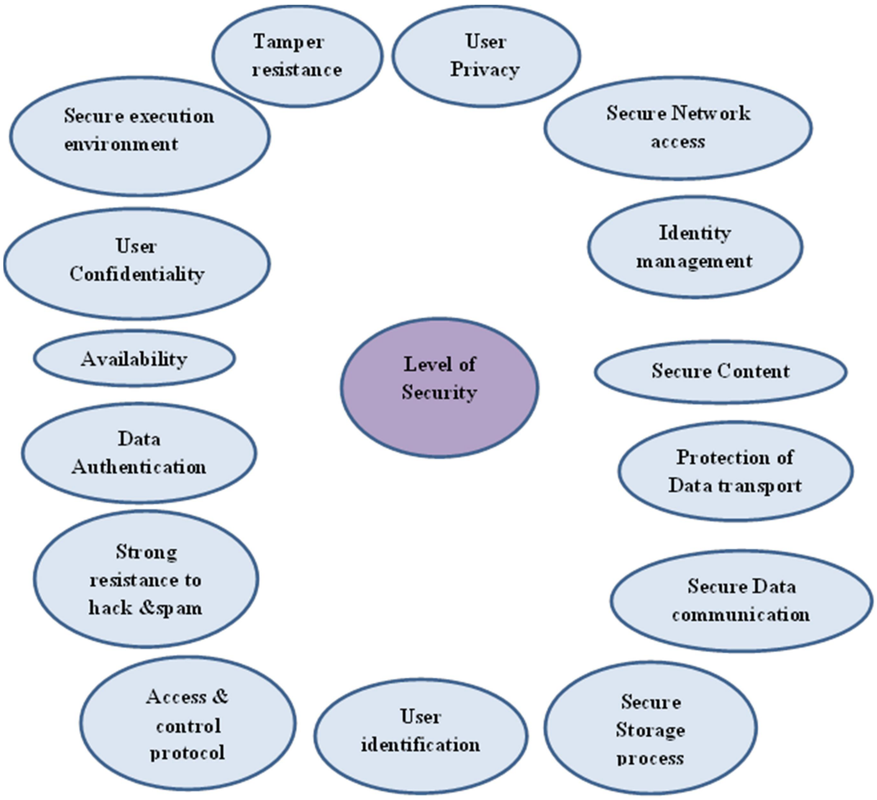

Figure 2. IoT Security Levels

1- User privacy

Any user has to be secured enough not to have his / her unified information scattered across unwanted part of a private e-LAN or the internet in general.

2- User confidentiality

This item controls the need and actions to be taken that the provider of services in an IoT is able to deduct from observing the use of the look-ahead system concerned with a specific user; at least, this deduction should be extremely difficult to take place.

3- Authentication of data

All data and packet data with received information from IoT devices and user side or, control units have to be authenticated.

4- Strong resistance to hack and spam attacks

The IoT systems should avoid having one point of failure and should be able to recover from nodes or multiple nodes failure, also avoid if necessary single points of failure.

5- Protocol for access and control

All information service providers must be able to adhere to access control protocols, to govern the way packets are retrieved and used within the network.

6- Protection of data transport

This part is usually deeply discussed ad portrayed by telecom protocols and its supporting security levels.

7-User identification

It refers to the action by which the user validating users takes place before granting access to the system.

8-Secure storage process

This involves confidentiality and access control of critical and sensitive parts of the packets and information that are stored in the network

9-Identity Management

It is a widely look up area that handles identifying people and their connected things in an IoT system and controlling their access to libraries and services within that system by linking user profiles and their access levels and with the created user rights

10-Secure data communication

This lists authenticating communicating peers, ensuring confidentiality and complex process of communication data, thus filtering loss of data transaction, hiding and protecting the user profile details of common communicating protocol.

11-Availability

Availability refers to complete allocation of authorized persons or systems, who can access the system or deny access or services to authorized users.

12-Secure network access

This provides a network connection or service services that can work only if the device is linked and validated.

13-Secure content

Content secure transaction is the key to secure IoT, namely, using Digital Rights Management (DRM) protects the rights of the digital files moving across the IoT system or network.

14-Secure execution environment

It refers to a secure, managed-application environment that is dedicated with a set of rules for preventing the system from hacks and attacks or suspicious applications.

15-Tamper resistance

The full protection to the IoT system even if the logical part is down, it can resists hacks even with a physical attempt or if the device falls with wrong hands or it receives threats from outside parties or hackers.

7. Securities and Threat Solutions for IoT

This section highlights some of the security and threat idioms for the IoT connected environment. Typically an IoT is connected to a set of devices that has its own security threats.

Meanwhile, the new algorithms or technologies in IoT security might be able to put some reliable solutions. Security threat level of IoT is a main topic that needs to be addressed and standardized. One typical example is how infinite its applications can be as it is basically linking or enabling devices to be smart and connected to the internet. There are few studies that proposed quantum cryptography (QC) for IoT as a robust security which can sustain the threats from the quantum computers such as (Routray et al., 2017). However, we can safely state that IoT is coupled with multiple security threats and alters overall information security risk profile, although the implementation of new protocols and restrictions may help IoT fight against threats and vulnerabilities. IoT security is basically, a data management topic and a highly rich research area. Effective management of these threats that are linked with IoT needs a deep and thorough risk evaluation, given the environment and development of a plan to go through clear and calculated risk. The various threats associated with the use of IoT (Herr et. al., 2015) are listed in the following paragraphs:

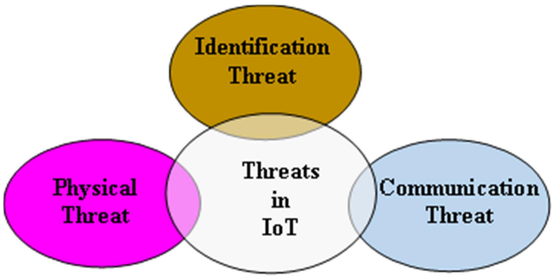

Figure 3. Threats Taxonomy for IoT

Identification threat covers determination of unique device/user/session with authentication, authorization, accounting, and provisioning.

Communication threat handles a Denial-of-Service attack (DoS) and it occurs when an attacker continually bombards a targeted AP (Access Point) or network with bogus requests, premature successful connection messages, failure messages, and/or other commands.

Physical threat includes micro probing and reverse engineering causing serious security problems by directly tampering the hardware components. Some types of physical attack require expensive material which makes them relatively hard to perform. Some examples are de-packaging of chip, Layout reconstruction, Micro-probing.

Embedded Security threat model will span all the threats at physical and MAC (Shih et al., 2001; Ye, Heidemann, & Estrin, 2002) layer. Security threats like device and data tampering, Side-channel analysis, bus monitoring, etc. will be the concerns at device level.

Storage management has a crucial impact on the key management to achieve confidentiality and integrity. We must also be careful in choosing which cryptographic components to use as the building blocks, for example, the cipher texts for some public key encryption.

The purpose of this research, as mentioned before, is to define and set up the basic building blocks of a secure IoT framework that allows providing mobile cloud services.

The main structure of the developed Secure Framework has two basic blocks: Certificate Generation and Authorization modules.

- Certificate Generation Module: This module is responsible for generating the certificate keys using keytool and storing them in the trust store database. This is shown in Figure 4.
- Authorization Module: It accepts the incoming service requests, analyzes the service name, host name, date validation of the certificate, if the certificate is self-signed or not, and the final check is its availability in the trust store or not. The request is rejected if it fails to satisfy the aforementioned requirements and it is accepted otherwise. This is shown in Figure 5.

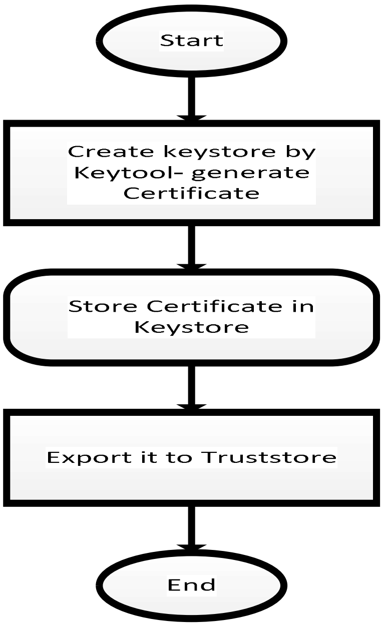
Start
Create keystore by Keytool- generate Certificate
Store Certificate in Keystore
Export it to Truststore
End

Figure 4.Certificate Generated by keytool

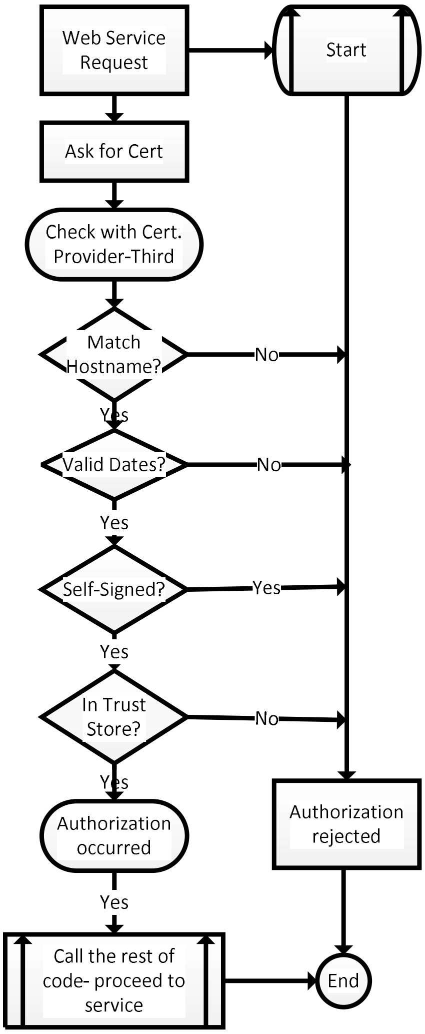

Figure 5. Certificate Authorization

8. Summary

The IoT (Atzori, et al., 2010) has immense potential to change many of our daily activities, routines, and behaviors. The pervasive nature of the information sources means that a great amount of data pertaining to possibly every aspect of human activity, both public and private, will be produced, transmitted, collected, stored and processed. Consequently, integrity and confidentiality of transmitted data, as well as the authentication of (and trust in) the services that offer the data, is crucial. Hence, security is a critical functionality for the IoT (https://en.wikipedia.org/wiki/Hype_cycle).

Wireless data networks are prone to a large number of attacks such as eavesdropping, spoofing, denial of service and so on. Legacy Internet systems mitigate these attacks by relying on link layer, network layer, transport layer or application layer encryption and authentication of the underlying data. Though some of these solutions are applicable to the IoT domain, the inherently limited processing and communication capabilities of IoT devices prevent the use of full-fledged security suites.

References

AlShahwan, F., & Faisal, M. (2016, 17-18 March). *Analyzing HTTP and COAP for IoT.* Paper presented at the Fourth International Conference on Advances in Computing, Communication and Information Technology CCIT- 2016 Birmingham, UK.

Amsalu, S. B., Zegeye, W. K., Hailemariam, D., & Astatke, Y. (2016, 16-18 March 2016). *Design and performance evaluation of an energy efficient routing protocol for Wireless Sensor Networks.* Paper presented at the 2016 Annual Conference on Information Science and Systems (CISS).

Aoudia, F. A., Gautier, M., Magno, M., Berder, O., & Benini, L. (2016). A Generic Framework for Modeling MAC Protocols in Wireless Sensor Networks. *IEEE/ACM Transactions on Networking*.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks, 54*(15), 2787-2805.

Bakht, M. P., & Shaikh, A. A. (2016). Routing Techniques in Wireless Sensor Networks: Review and Survey. *Journal of Applied and Emerging Sciences, 6*(1), pp18-23.

Bormann, C., Castellani, A. P., & Shelby, Z. (2012). CoAP: An Application Protocol for Billions of Tiny Internet Nodes. *IEEE Internet Computing, 16*(2), 62-67.

Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: a survey. *Future generation computer systems, 56*, 684-700.

Crooks, A., Schechtner, K., Dey, A. K., & Hudson-Smith, A. (2017). creating smart Buildings and cities. *IEEE Pervasive Computing, 16*(2), 23-25.

GAO, L.-j., & CHEN, Z.-g. Security in Next-Generation Wireless Sensor Networks.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems, 29*(7), 1645-1660.

Hara, S., Zhao, D., Yanagihara, K., Taketsugu, J., Fukui, K., Fukunaga, S., et al. (2005). *Propagation characteristics of IEEE 802.15.4 radio signal and their application for location estimation* (Vol. 1).

Hasan, M. Z., Al-Rizzo, H., & Al-Turjman, F. (2017). A Survey on Multipath Routing Protocols for QoS Assurances in Real-Time Wireless Multimedia Sensor Networks. *IEEE Communications Surveys & Tutorials*.

Herr, D. A., Kassimis, C., & Stevens, J. W. (2015). Protocol selection for transmission control protocol/internet protocol (tcp/ip): Google Patents.

Hype Cycle from https://en.wikipedia.org/wiki/Hype_cycle

Juels, A. (2012). RFID security and privacy: Springer.

Li, S., Da Xu, L., & Zhao, S. (2015). The internet of things: a survey. *Information Systems Frontiers, 17*(2), 243.

Negi, V. (2014). from https://www.slideshare.net/vikrantnegi007/internet-of-things-seminar

Routray, S. K., Jha, M. K., Sharma, L., Nyamangoudar, R., Javali, A., & Sarkar, S. (2017, 19-20 May 2017). *Quantum cryptography for IoT: APerspective.* Paper presented at the 2017 International Conference on IoT and Application (ICIOT).

Shahid, R., Simon, D., Joel, H., Utz, R., & Thiemo, V. (2014). Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN. *Security and Communication Networks, 7*(12), 2654-2668.

Shih, E., Cho, S.-H., Ickes, N., Min, R., Sinha, A., Wang, A., et al. (2001). *Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks.* Paper presented at the Proceedings of the 7th annual international conference on Mobile computing and networking.

Streitz, N., & Markopoulos, P. (2016). *Distributed, Ambient and Pervasive Interactions: 4th International Conference, DAPI 2016, Held as Part of HCI International 2016, Toronto, ON, Canada, July 17-22, 2016, Proceedings* (Vol. 9749): Springer.

Sudarshan, S. K., Khan, M. S. A., Dao, K., & Pham, T. A Comprehensive Study of Mobile Sensing and Cloud Services.

Tomar, G. S., Chaudhari, N. S., Bhadoria, R. S., & Deka, G. C. (2016). *The Human Element of Big Data: Issues, Analytics, and Performance*: CRC Press.

Urzaiz, G., Hervas, R., Fontecha, J., & Bravo, J. (2016). *The Advanced Network of Things: A Middleware to Provide Enhanced Performance and Functionality in IoT.* Paper presented at the Ubiquitous Computing and Ambient Intelligence: 10th International Conference, UCAmI 2016, San Bartolomé de Tirajana, Gran Canaria, Spain, November 29–December 2, 2016, Part II 10.

Woo, A., & Culler, D. E. (2001). *A transmission control scheme for media access in sensor networks.* Paper presented at the Proceedings of the 7th annual international conference on Mobile computing and networking.

Ye, W., Heidemann, J., & Estrin, D. (2002). *An energy-efficient MAC protocol for wireless sensor networks.* Paper presented at the INFOCOM 2002. Twenty-first annual joint conference of the IEEE computer and communications societies. Proceedings. IEEE.

Feda AlShahwan is currently an Assistant Professor at the Electronic Engineering Department/Computer Section of the College of Technological Studies in the Public Authority for Applied Education & Training. She has diverse research interests in Mobile Web Services and their applications Born in Kuwait, obtained her B.Sc., M.Sc. in Computer Engineer from Kuwait University 1992, 2004 respectively. She had her Ph.D. in “Adaptive Service Provision and Execution in Mobile Environments” from Centre for Communications Systems Research in University of Surrey. Her current research interests include studies of Adaptive Mobile Web Services, Social networks, Internet of Things, MANET and Mobile Cloud Computing.

Maha H. Faisal received her Ph.D. from the University of Colorado at Boulder in 2005. Dr. Faisal is currently an assistant professor at the Computer Engineering Department, Kuwait University. Her research interests include human computer interaction, computer mediated social interaction, pervasive computing and software system modeling.