ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

Security Mechanisms for IOT Services and Differences between IOT and Traditional Networks

Adithya Vuppula

Full Stack Developer, Marlabs Inc., Piscataway, New Jersey, USA

ABSTRACT: It is expected that by 2020 tens of billions of things will be deployed worldwide. It became evident that the traditional centralized computing and analytic approach does not provide a sustainable model this new type of data. A new kind of architecture is needed as a scalable and trusted platform underpinning the expansion of IoT. The data gathered by the things will be often noisy, unstructured and real-time requiring a decentralized structure storing and analyzing the vast amount of data. This paper provides a detailed study on the differences between iot and traditional network.

KEYWORDS: Internet of Things, security mechanisms, IoT services

I. INTRODUCTION

In low and middle income countries, there is increasingly growing number of people with chronic diseases due to different risk factors such as dietary habits, physical inactivity, and alcohol consumption among others. According to the World Health Organization report, 4.9 million people die from lung cancer from the consumption of snuff, overweight 2.6 million, 4.4 million for elevated cholesterol and 7.1 million for high blood pressure [1]. Chronic diseases are highly variable in their symptoms as well as their evolution and treatment. Some if not monitored and treated early, they can end the patient's life.

For many years the standard way of measuring glucose levels, blood pressure levels and heart beat was with traditional exams in a specialized health centers. Due to the technological advances in today, there is great variety running sensor reading vital signs such as blood pressure cuff, glucometer, heart rate monitor, including electrocardiograms[2], which allow patients to take their vital signs daily. The readings which are taken daily are sent to doctors and they will recommend the medicine and workout routines that allow them to improve the quality of life andovercome such diseases.

The internet of things applied to the care and monitoring of patients is increasingly common in the health sector, seeking to improve the quality of life of people. The Internet of things is defined as the integration of all devices that connect to the network, which can be managed from the web and in turn provide information in real time, to allow interaction with people they use it [3]. On the other hand, the Internet of things can be seen from three paradigms[4], which are Internet-oriented middleware, things sensors oriented and knowledge-oriented semantics.

The arduino is a programmable device that can sense and interact with its environment. It is great open source microcontroller platform that allows electronic enthusiasts to build quickly, easily and with low cost small automation and monitoring projects. The combination of IoT with arduino is the new way of introducing Internet of Things in Health care Monitoring system of patients[5]. Arduino Uno board collects data from the sensors and transfer wirelessly to IoT website.

The Internet can be described as the communication network that connects individuals to information while The

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

Internet of Things is an interconnected system of distinctively address able physical items with various degrees of processing, sensing, and actuation capabilities that share the capability to interoperate and communicate through the Internet as their joint platform [1]. Thus, the main objective of the Internet of Things is to make it possible for objects to be connected with other objects, individuals, at any time or anywhere using any network, path or service. The Internet of Things is gradually being regarded as the subsequent phase in the Internet evolution. IoT will make it possible for ordinary devices to be linked to the internet in order to achieve countless disparate goals. Currently, an estimated number of only 0.6% of devices that can be part of IoT has been connected so far [2]. However, by the year 2020, it is likely that over 50 billion devices will have an internet connection.

As the internet continues to evolve, it has become more than a simple network of computers, but rather a network of various devices, while IoT serves as a network of various "connected" devices a network of networks [3], as shown in Fig. 1. Nowadays, devices like smartphones, vehicles, industrial systems, cameras, toys, buildings, home appliances, industrial systems and countless others can all share information over the Internet. Regardless of their sizes andfunctions, these devices can accomplish smart reorganizations, tracing, positioning, control, real-time monitoring and process control. In the past years, there has been an important propagation of Internet capable devices. Even though its most significant commercial effect has been observed in the consumer electronics field; i.e. particularly the revolution of smartphones and the interest in wearable devices (watches, headsets, etc.), connecting people has become merely a fragment of a bigger movement towards the association of the digital and physical worlds.

With all this in mind, the Internet of Things (IoT) is expected to continue expanding its reach as pertains the number of devices and functions, which it can run. This is evident from the ambiguity in the expression of "Things" which makes it difficult to outline the ever-growing limits of the IoT [4]. While commercial success continues to materialize, the IoT constantly offers a virtually limitless supply of opportunities, not just in businesses but also in research. Accordingly, the understudy addresses the various potential areas for application of IoT domains and the research challenges that are associated with these applications.

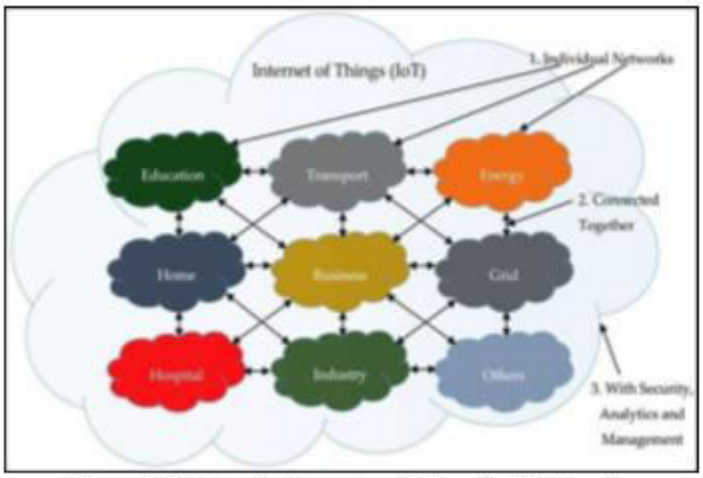

Figure 1: IoT can be viewed as a Network of Networks.

II. DIFFERENCES BETWEEN IOT AND TRADITIONALNETWORK

In the beginning, the IoT technology has broken a lot of the traditional ideas of network and started a new era of telecommunication technology. Can be considered IoT as an extension and expansion network based on the Internet; but it is different from either traditional network or the so- called Internet of people and WSN although

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

considered as backbone to build any IoTblock.

The major equation to represent the IoT environment is *"IoT environment= Internet + WSN",* it is a common statement that uses to express the IoT environment. To analyze and judge the correctness of this statement, must be determined the similarities and differences between IoT, Internet, and WSN according to table 1.

From the previous knowledge about the IoT environment can be judged on this view, it's a wrong; because there are two basic reasons for rejecting this view. First; IoT may not necessarily use IP in all cases for addressing things, because nature of IoT needs lightweight communication protocols, the complexity of the TCP/IP protocol is not suitable in particular, when works with the smart little things. Second, the IoT environment is mainly based on the connected smart objects unlike traditional network. That's what makes them move from only a mere extension of the Internet, also the behavior of IoT depends on the creation of the interoperable systems, based on these arguments, can be corrected the previousstatement:

IoT= Internet + WSN+ Smart Items surrounded by Intelligent environment.

Finally, IoT supports a set of useful features such as interoperability, self- configuration, self- adaptive and self-protection. The intelligent environment is a way to ensure the existence of a minimum level of the previously mentioned elements within the network.

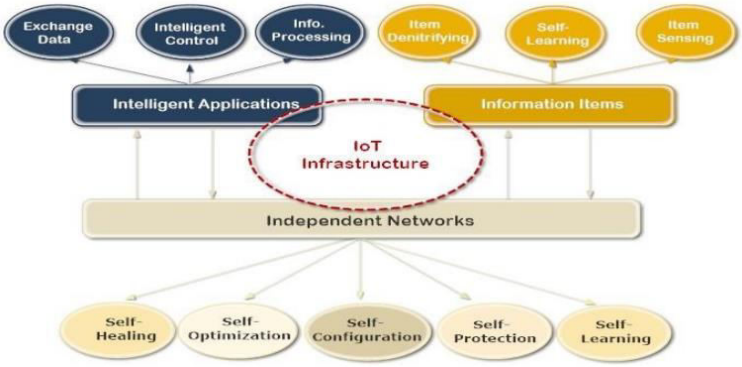

Figure 2: The three Dimensions of IoT

Characteristics		Internet	WSN
Comm. Protocol	Lightweight Comm. protocols.	(TCP/IP)	Lightweight Comm. protocols.
Scale degree of Area	Cover wide area	Cover wide area	Cover local area
Networking Approach	Determine backbone	Determine backbone	Self-organization
Identify objects	Must	Can not	Can
Type of nodes	Active and passive	Active	Active
Network design	WSN+ dynamic smart things+Internet surrounded by intelligent environment	Set of networks contains set of Fixed objects	Dynamic smart objects
Behavior	Dynamically	Fixed	Dynamically
Networking Time	Timing synchronization	Unlimited	Unlimited

Table 1: The similarities and differences between IoT, Internet, and WSN

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

III. MAIN SECURITY MECHANISMS FOR IOT SERVICES

Cryptography

Securing data such as user identities, bank credit card numbers, etc. is referred to as Cryptography, using cryptographic algorithms to relay these messages across the network. In network defense, several encryption algorithms are used. Symmetric, public-key, and Cryptographic protocols are split into three basic groups. They are categorized as: Symmetric algorithms where one key is used to encrypt and decrypt data that use two keys, i.e. private and public keys, Depending on the amount of keys that are used for encryption and decryption. For encryption, the public key is used, and the private key is used for decryption. Rivest-Shamir-Adelman, Data Encryption Standard, Advanced Encryption Standard are some of the essential cryptographic algorithms accessible. While these algorithms are important for information technology security, a large range of computational resources, such as time for the CPU, storage and batteries energy, are consumed. Based on the key size used, the strength of symmetric key encryption varies. In addition, Unclassified information is protected from attackers by using the DES algorithm that uses the same key for encryption and decryption operations.

Lightweight cryptography

Lightweight block ciphers work with a transformation defined by a symmetric key on fixed- length bits. This flexible primitive uses more complex operations and is implemented using the substitution and permutation networks. SPN includes a number of rounds of substitute boxes and permutation boxes generating a network to create a cipher text block, which then applies a plaintext block and key to mathematical operations. The advantage of the symmetric nature of the Cipher text is that the processes of encryption and decryption are almost equivalent, divided by the opposite of the key schedule. The nearly halved size of the requisite code or circuitry may then be comfortably added. The very low latency of lightweight block ciphers. Based on the design of the restrictions they begin to solve, such as length, speed or energy, lightweight blocks may usually be designed for various things. PRESENT, KLEIN and ZORRO are three of these light-weight block ciphers. PRESENT was already developed and applied successfully in hardware that can be designed to have a very low number of gates.

Hardware security

There are several important limitations to hardware-based security primitives and protocols. Three are dominant among them. It's just that Silicon Physical Unlovable Functions appeared as a successful basic hardware security with a growth potential for Radio Frequency Identification tags, safety communication protocols, Core network defense, collection of cryptographic key, user authentication of applications, before the advent of the public physical feature. The procedure has very limited hardware for processing and no operational expenses for slowdown and energy. The key idea would be to include only a limited subset of concerns, but it is dependable under a wide range of circumstances. While the multitude of issues used is drastically diminished from the initial amount of challenges, the number of items used for problems is still increasing in their cardinality. This method extends many different structures. Primitive optical hardware protection is the second. It is an electronic signal with very small gate amounts, high throughput, and super energy requirements, but it is initialized using stable analog. The protected and trusted flow of information, the removal of side channels and the latency of just a few gate numbers of public key security protocols can therefore be directly combined with standard digital designs and facilitated.

Random number generator

In general, A black box that takes input and generates incoming messages within a specified range is a random number generator. Pseudo-RNGs and True-RNGs are classified into two main groups. Pseudo-RNGs are easy to execute and suitable for many applications, and a TRNG is often required, particularly for super accurate systems. The reason for

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

this is that PRNG was built from a computing algorithm which has testable properties. It also destroys the random number it generates since the code behind the PRNG is broken. A True-RNG, from the other side, a concrete structure that has inherent randomness is used to produce a RNG that can be extracted. This refers to non properties in the case of TRNG. However, these systems have limited randomness and can be easily dominated, achieve data security against cyber-attacks. Their unpredictability makes TRNG based on hardware more stable than PRNG based on software.

IV. CONCLUSION

The key idea to gain the smart environment such as smart city or smart home while maintaining the level of service without degradation has relied on the integration between both IoT and cloud computing; over recent year's escalation of attention toward this integration. Generally, The IoT suffers from a host of the thorniest issues, first of all, heterogeneity of objects; there are many middleware technologies are designed to deal with this type of issues, such as RFID middleware and WSN middleware. On the other hand,the cloud computing provides scalability and hide complexity of sensors from end users by using the virtualization technology. This paper provided a detailed study on the differences between iot and traditional network.

REFERENCES

1. Purnima, Puneet singh, "Zigbee and GSM based Patient Helath Monitoring System", IEEE International Conference on Electronics and Communication System, September 2014.
2. MatinaKiourexidou, Konstantinos Natsis, Panagiotis Bamidis, NikosAntonopoulos, EfthymiaPapathanasiou, Markos Sgantzos, Andreas Veglis "Augmented Reality for the Study of Human Heart Anatomy" International Journal of Electronics Communication and Computer Engineering 2016.
3. Sankar Kumar S, Gayathri N , Nivedhitha D , Priyanka A S "A Cost effective Arduino Module for Bedridden patient's Respiratory Monitor and Control" International Journal of advanced research trends in engineering and technology (IJARTET) VOL. II, SPECIAL ISSUE XXI, MARCH 2016.
4. Bhagya Lakshmi, M1 Hariharan ,R2 Udaya Sri, C3 Nandhini Devi, P4 Sowmiya"Heart Beat Detector using Infrared Pulse Sensor" IJSRD - International Journal for Scientific Research & Development| Vol. 3, Issue 09, 2015.
5. Ch.Sandeep Kumar Subudhi,'Intelligent Wireless Patient Monitoring and Tracking System (Using Sensor Network and Wireless Communication)",2014.