ISSN(Online) : 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2014

Communication and Protocols towards IOT-Based Security

Adithya Vuppula

Student, Bachelor of Technology in Computer Science, SR Engineering College (JNTU affiliated), India

ABSTRACT: IOT devices are used in many application fields which make the users' day to day life more comfortable. These devices are used to collect temperature, blood pressure, and sugar level etc., which are used to evaluate the health condition of the patient. Communicating the collected information to the doctor, making accurate decision on the data collected and notifying the patient is the challenging task in the IOT. In this project, An IoT based Patient Health Monitoring System using Arduino is proposed to collect the required parameters and evaluate the data obtained from the sensor devices. PHMS with arduino also gives the notifications to patient with possible precautionary measures to be practiced by them. This system suggests the patient with medical care and next step to be followed in case of critical situation. The combination of IoT with arduino is the new way of introducing Internet of Things in Health care Monitoring system of patients. Arduino Uno board collects data from the sensors and transfer wirelessly to IoT website. This paper provides the architectures, design, security communication and protocols towards internet of things.

KEYWORDS: Internet of Things, security communication, protocols

I. INTRODUCTION

Smart devices. Smartphones. Smart cars. Smart homes. Smart cities. A smart world. These notions have been espoused for many years. Achieving these goals has been investigated, to date, by many diverse and often disjoint research communities. Five such prominent research communities are: Internet of Things, Mobile Computing, Pervasive Computing, Wireless Sensor Networks, and most recently, Cyber Physical Systems. However, as technology and solutions progress in each of these fields there is an increasing overlap and merger of principles and research questions. Narrow definitions of each of these fields are no longer appropriate. Further, research in IoT, PC, MC, WSN and CPS often relies on underlying technologies such as real-time computing, machine learning, security, privacy, signal processing, big data, and others. Consequently, the smart vision of the world involves much of computer science, computer engineering, and electrical engineering. Greater interactions among these communities will speed progress.

Internet of Things (IoT) has emerged strongly as a more prosperous area to express this kind of a new technology. It is not the first technology in this field, but also the cloud computing technology has been used to represent the ubiquitous computing world. In the seventh in the series of ITU Internet Reports originally it was launched in 1997 under the title "Challenges to the Network" [1], and it was first coined by Kevin Ashton in the RFID journal 1999 [2], In 2005 this name was changed to "Internet of things". The vision of IoT according to Kevin's vision was to enable networked devices to propagate their information about physical world objects through the web. In recent years, the most of the IoT proposed architectures are used, web semantic to publish information through the social networks; for instance, the iPhone has innovated service is Nike + iPod to record information and published it on the social networks and the social network friends [3].

The most popular and practical online system is the Internet of Things. It links to the Internet with different sensors and controllers and helps to achieve direct communication between individuals and things. The main future of the Internet appears to be that. The quantity and variety of devices have grown quickly, With the strength of the IoT industry, particularly in previous seasons. The IoT devices share a similar architectural style. Under this framework, each layer (edge, middleware, and application) carries its collection of security risks that must be taken into account. In addition,

DOI: 10.15680/IJIRSET.2014.0310093

ISSN(Online) : 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2014

Large combinations in development tools make IoT protection a difficult issue to address. For this purpose, it will help their adoption and future product iterations to create a well-defined security model for IoT devices. IoT, like more vulnerabilities and security threats, presents pressing security challenges. It also need new and smarter IoT security approaches, in particular approaches capable of handling complex, unpredictable and often asymmetric threats on a scale. In addition, interconnected devices have a direct effect on the lives of users, new technologies and protocols require a well-defined classification of security threats and a proper security structure that can mitigate security challenges in terms of privacy, data integrity, and IoT availability. Cyber-attacks targeting it are growing as IoT devices become popular. And these attacks, both at home and around the world, create business and operation delays, intelligence leaks, and financial damage, disrupting economic growth and the safety and security of regular activities. Cyber-attacks on IoT devices result in financial and social disruption, social awareness with the need for IoT device security will further expand. A massive amount of data creates by The Internet of Things is a big challenge to be handled, other obstacle includes the limitation of the current network structure that are incapable to handle real-time sensitive applications using IoT, therefore Software Defined Networking is expected to be a suitable network infrastructure for such applications. This paper's contents will be organized as follows: section 2 presents brief information about security aspects, section 3 presents an IoT layers and security theaters, section 4 Security mechanisms for IoT services, section 4 describes IoT protocols and communication, and finally, section 5 provides a description and ideas for possible directions for research about IoT protocols.

Actually, the definition of IoT varies based on who you talk, but formally, it can be defined as a dynamic global network infrastructure with self-configuration and interoperable communication. Simply, IoT means the ability to make everything around us starting from (i.e. Machine, Devices, Mobile phone and Cars) even (Cities and Roads) are expected to be connected to the Internet with an intelligent behavior and taking into account the existence of the kind of autonomy and privacy. Meanwhile, the IoT environment contains a huge number of the different objects/things can be classified into two types namely; i) Things rechargeable batteries things: the most of them are mobiles (e.g. Laptop, tablets and mobile phone), and ii) Things are non-rechargeable things: these things are static from the mobility point of view [4]. Generally, IoT includes three main demands are: the first, a shared understanding of the situation of its users and their applications. Secondly, software architecture and pervasive communication networks to cover and process contextual information, and lastly, the analytics tools in IoT that aims for autonomous and intelligent behavior [5].

Considerably, can be expressed the principle idea of IoT is promoting the communication between anything from anywhere at anytime through context-aware applications. Accordingly, IoT has relied on RFID and sensor network technologies in the implementations. For instance, IBM company used IoT in Norwegian Sea oil platforms, by deploying sensors at seabed that are used to collect real information to make decision drill in the sea [3].

On the other hand, the IoT environment like many networks suffering from the set of challenges which significantly affect their performance some of them are common and others, are special; the paper divides these challenges into two categories, namely, i) General challenges: which include common challenges between IoT and traditional network such as communication, heterogeneity, QoS, scalability, virtualization, data mining and security; and ii) Special challenges: such as RFID and WSN.

II. LITERATURE SURVEY

[1]: This paper reviews the current research of IoT, key enabling technologies, major IoT applications in industries, and identifies research trends and challenges. A main contribution of this review paper is that it summarizes the current state-of-the-art IoT in industries systematically.

[2]: This paper presents framework for realizing energy efficient smart homes based on wireless sensor networks and human activity detection. Their work is based on the idea that most of the user activities at home are related to a set of electrical appliances which are necessary to perform these activities. Therefore, they show how it is possible to detect the user's current activity by monitoring his fine-grained appliance- level energy consumption. This relation between activities and electrical appliances makes it possible to detect appliances which could be wasting energy at home. Our

DOI: 10.15680/IJIRSET.2014.0310093

ISSN(Online) : 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2014

framework is organized in two components. On one hand, the activity detection framework which is responsible for detecting the user's current activity based on his energy consumption.

[3]: This paper surveys the existing works on occupancy monitoring and multi-modal data fusion techniques for smart commercial buildings. The goal is to lay down a framework for future research to exploit the spatio-temporal data obtained from one or more of various IoT devices such as temperature sensors, surveillance cameras, and RFID tags that may be already in use in the buildings.

[4]: This paper focuses specifically to an urban IoT system that, while still being quite a broad category, are characterized by their specific application domain. Urban IoTs, in fact, are designed to support the Smart City vision. This aims at exploiting the most advanced communication technologies to support added-value services for the administration of the city and for the citizens. This paper hence provides a comprehensive survey of the enabling technologies, protocols, and architecture for an urban IoT.

[5]: This paper provides an overview of the Internet of Things (IoT) with emphasis on enabling technologies, protocols, and application issues. The IoT is enabled by the latest developments in RFID, smart sensors, communication technologies, and Internet protocols. The basic premise is to have smart sensors collaborate directly without human involvement to deliver a new class of applications. The current revolution in Internet, mobile, and machine-to- machine technologies can be seen as the first phase of the IoT. In the coming years, the IoT is expected to bridge diverse technologies to enable new applications by connecting physical objects together in support of intelligent decision making. This paper provides a horizontal overview of the IoT. Then give an overview of some technical details that pertain to the IoT enabling technologies, protocols, and applications. Compared to other survey papers in the field, our objective is to provide a more thorough summary of the most relevant protocols and application issues

III. ARCHITECTURES AND DESIGN

A scaleable and reliable architecture will form the backbone of the future development of IoT. The architecture must cope with the new requirements of IoT and reflect the challenges listed in Section II. This Section covers the architecture reference model IoT-A, as well as two full-fledged architectures developed in the projects BETaaS and OPENIoT.

A. IoT-A

The IoT Architecture Reference Model is not an IoT architecture per se, but a set of best practices, guide- lines, and a starting point to generate specific IoT architectures. It provides an architectural reference model facilitating the interoperability of IoT systems. It also provides the tools, such as resolution, look up, and discovery of things, for the actual integration into the service layer.

The ARM Process defines the steps to generate concrete IoT architectures from business goals, informing on IoT related issues in a methodology agnostic way. The covered topics include the generation of requirements and their transforma- tion into an architecture using views and perspectives. ARM provides an exhaustive list of so-called Unified Requirements, that can be used to generate concrete require- ments for a specific architecture. The UNIs are generalized requirements augmented with the views and perspectives of the respective stakeholders.
The ARM process makes use of the IoT Reference Model that introduces major IoT concepts such as devices, services, and entities and defines their relations and attributes on an abstract level that is independent from specific use cases or technologies. Following the established relations, it identifies so-called Functional Groups for interacting with in- stances of the introduced concepts and introduces communi- cation functionalities suitable for heterogenous IoT settings. Additional features introduced include trust, security, process management, service organization, and more.

B. BETaaS

Building the Environment for the Things as a Service defines besides the overall functionality and architecture, an actual implementation of the platform is part of the deliverables. BETaaS is a running project and some deliverables are not yet available in their final version or are even still missing completely. BETaaS consists of a network of gateways ("local cloud of gateways") that seamlessly integrate existing heterogeneous M2M systems. To abstract from the heterogeneity of the physical layer, BETaaS defines and builds upon a baseline reference architecture called Things-as-a-Service. The TaaS Reference Model is the foundation of the BETaaS infrastructure on which it is built. It provides architectural models for

DOI: 10.15680/IJIRSET.2014.0310093

ISSN(Online) : 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2014

domains, information, communication, security, and functions. TaaS builds upon the IoT-A models, tailoring and extending them to its specific needs.

C. OPENIoT

The OPENIoT research project has defined an architecture utilizing a Sensor Middleware and a Semantic Directory Service. To achieve alignment, architecture development and specification was based on the Architecture Reference Model of IoT-A.

The Sensor Middleware undertakes the collection, filtering and aggregation of data streams associated to physical and virtual objects. The Cloud Computing Infrastructure supports the storage of data along with their associated meta- data information in a scalable and elastic manner. The Seman- tic Directory Service supports registration management and semantic annotation for sensors and services. The Global Scheduler is tasked with handling requests for on-demand service deployment and the associated provisioning of access to data sets and services that may be required. The Request Definition element enables the dynamic specification of service requests and the Request Presentation element is tasked with the visualization of the results produced by an executing service.

The best design of the architecture is a foundation stone to build a privileged IoT system; this architecture helped to address a lot of issues in the IoT environment such as scalability, routing, networking, etc.. Typically, the IoT architecture approach based on three main dimensions are:

i.Information items: it includes all items connected to IoT environment may be sensing items, identifying items and control items; ii) Independent network: which includes several features such as self-configuration, self-protection, self-adaptation, and self-optimization; and iii) Intelligent applications: which have intelligent behavior over the Internet generally; the intelligent behavior may be intelligent control, exchange data methods through network items, data processing, all the applications which are related to the IoT can be classified according to these dimensions [9]. The intersection between these dimensions creates a new space named “infrastructure of IoT”, which provides support systems to serve the special things, which can provide various services such as goods identification, location identification and data protection.

In this end, There are several approaches to build an architecture of IoT, the paper will focusing on two kinds namely, architecture called “EPC global network“ and another called “Unite and ubiquitous IoTs or U2IoTs”, to create an application on IoT, the architectural approach favored which based on an open architecture the EPC global network. The system designed by AutoID center for conveying the dynamic information about objects/things to provide a history of the product movement for the authorized users, the RFID technology plays a key role to differentiate between these mobile objects, this system is called “the EPC global network”. The IoT uses the EPC global network as a principle to design the architecture framework.

The future architecture of IoT seeks to achieve connection between real-world, cyber-world and social world. Unite and ubiquitous IoTs or U2IoTs is considered as a different kind of IoT architecture, it’s used to integrate the physical world with the cyber world. The U2IoTs consists of a set of heterogeneous systems, including unit of IoT to resemble human neural network that provides solutions to specific applications; U2IoTs includes the industrial IoT, local youth, national IoT, and global IoT which integration of multiple Unit IoTs with ubiquitous features, and it is similar to the social organization framework. The main characteristics of U2IoT model are cyber, physical, social co-existence, connectivity and interactivity, space-time consistency and multi-identity status.

IV. IOT-BASED SECURITY COMMUNICATION AND PROTOCOLS

ZigBee

ZigBee is a wireless and based on the IEEE 802.15.4 standard. It was launched in 2004 by the ZigBee Alliance and in the form of. Primarily defined by very low powered demands and lower utilization speeds.

1. The protocol can reduce the battery replacement speed and has a transfer rate of up to 25000 bps, with a range of up to 1 kilometer. In the ZigBee protocol, safety assumes a key role. The Advanced Encryption Standard is the encryption algorithm

ISSN(Online) : 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2014

used in ZigBee. Such a highly stable and accurate algorithm ensures the secrecy and reliability of wireless communications. Two separate security models are given by ZigBee: standard security model, implemented simple security model due to its vulnerability to threats, and High Security, each of which is used because it guarantees better security during communications. If data is unencrypted on a ZigBee network, a hacker can control all network information and can also sniff/capture packets that have been transmitted. Instead, if communication is protected, an unauthorized attacker may only execute attacks that do not enable network access, It is very hard to observe the network key supported by ZigBee and decipher the messages sent, including access denial or bumping. The AES 128-bit encryption algorithm is implemented by ZigBee security, which also provides security resources such Key transmission, structure security and device control, as key generation. Each layer responsible for uniqueness frame is responsible for automatically swapping the key for each input and output node, and without the need to decrypt and encrypt, data is transmitted at each step. Security features provided by the ZigBee standards will be covered, including in the sense of secure sets and strong encryption.

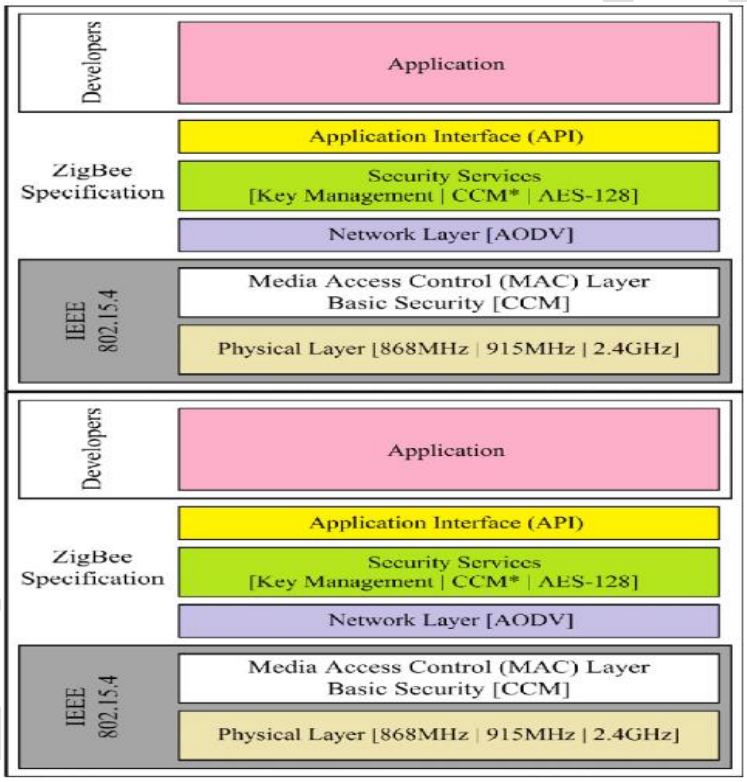

Figure 1: ZigBee stack

ZigBee Networks are subject to multiple kinds of attacks. In keeping with the safety criteria of ZigBee Networks, This attacks can be grouped into five kinds of attacks:

Eavesdropping: An external attack in which an hacker may attempt to passively overhear or listen to the conversation on the network and take the data.

Denial of Service: That arise when hackers use a PC to send movements with the ultimate aim of interfering with the network's radio frequencies (2.4 GHz). This kind of DoS can also be found on the data link layer where, for example, IEEE 802.15.4 or ZigBee, have a particular mission to interrupt the communication protocols.

Node Compromise: It is a sort of act by which an attacker catches and exploits or reprogrammed a valid node in the network.

DOI: 10.15680/IJIRSET.2014.0310093

ISSN(Online) : 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2014

Sinkhole and Wormhole: It is a situation in which the malware network device by spreading fake routing data gathered packets to it, which in turn upsets the network's routing operation. In a Wormhole Attack, an attacker gathers packets for one network connection, passes them to another place of the network, and then replays them into a network to generate confusion about the routing, forwarding and other significant actions of the node.

Physical Attack: The attacker's ability to obtain physical access to a network device.

Bluetooth low energy

Unlike standard Bluetooth, BLE is designed for sensor networks with a small data rate of up to 1 Mbit/s, with an emphasis on power efficiency, it was released and BLE is conflicting with Bluetooth Classic. Both run in the 2.4 GHz frequency range with a separate range of wavelength channels. The software is supported and distributed by the Bluetooth SIG. BLE specifies a set of software features that can be applied by devices. A model is a collection of services that a system offers and, including its purpose, each machine may introduce a variety of modules. BLE has so far been restricted to linking only two devices. The Mesh interface was implemented by Bluetooth SIG, making multi-to-many connectivity. Encrypted data is optional in BLE and is performed during the connected components' matching process. Exchanging the encryption key is a critical part of protecting the connection. The joining method is a key contributor to Bluetooth security problems. During various phases of the connection process, attacks can be carried out, both before the matching process is finished and after the devices are matched. Pairing in BLE is not considered stable up to version 4.1, since there is no eavesdropping security that can lead to key loss. The risk of requiring linking devices to regenerate their keys makes this much more risky. In addition, The common keys will have a negotiable length of almost as 7 bytes and the amount of authentication issues is endless. Encryption and other authentication enhancements remain optional except with the changes in later releases and are not introduced by many vendors. On the application layer, some suppliers impose encryption, but application vulnerabilities or poor security against particular threats are very popular. Finally, while all the encryption keys of the BLE standard are used correctly by the vendor, it does not ensure quality. The flexibility of the design which contributes to defects in security created by a procedure, including big limitations such as arbitrary code execution.

V. CONCLUSION

Despite of fast and vast growing in this area it faces the main issue which is the security of the devices and users. Because of the security vulnerabilities will bring serious dangers to users' security and property this paper discusses the main challenges and solution in this field. This paper discusses and examines the main IoT protocols that used to communicate between IoT based devices and their vulnerabilities and weaknesses to the attackers. Starting from LoRaWan which uses 128 AES key in C-Media Access Control mode and 6LWPAN which implements authentication and authorization between the clients during the transmission, ending with BLE and Zigbee, the first one the programmer should be aware to authenticate the users in each stage while the latter one works like Bluetooth by applying pairing technique between clients. his paper provided the architectures, design, security communication and protocols towards internet of things.

REFERENCES

1. Atzori, L., Iera, A., Morabito, G., Nitti, M.: The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization. Computer Networks 56(16), 3594–3608 (2012)
2. Bauer, M., Boussard, M., Bui, N., De Loof, J., C., M., Meissner, S., Nettsträter, A., Stefa, J., Thoma, M., Walewski, J.W.: IoT Reference Architecture. In: Enabling Things to Talk: De- signing IoT solutions with the IoT Architectural Reference Model. Springer Berlin Heidelberg (2013)
3. Bonomi, F., Milito, R., Natarajan, P., Zhu, J.: Fog Computing: A Platform for Internet of Things and Analytics. In: Big Data and Internet of Things: A Roadmap for Smart Environments, pp. 169–186. Springer (2014)
4. Borgia, E.: The Internet of Things vision: Key features, applications and open issues. Computer Communications 54, 1–31 (2014)

DOI: 10.15680/IJIRSET.2014.0310093