IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

A Review on IoT - Technology, Application, Architecture, Services

Mohammed Anwaruddin[1], Mohd. Abdul Sattar[2], Mohd. Anas Ali[3]

Assistant Professor, Dept. of ECE, Nawab Shah Alam Khan College of Engineering & Technology, Hyderabad, India[1,3]

Associate Professor, Dept. of ECE, Nawab Shah Alam Khan College of Engineering & Technology, Hyderabad, India[2]

Abstract: The "internet of things" (IoT) concept is used to define or reference systems that rely on the autonomous communication of a group of physical objects. The applications areas of the IoT are numerous, including: smart homes, smart cities and industrial automation. IoT systems often provide great benefits to numerous industries and society as a whole. Many of the IoT systems and technologies are relatively novel. The aim of this paper is to provide the last and most innovative contributions concerning the Protocol, Technology, Application, Architecture & Issues of interest in IoT solutions that involve interconnected smart things that interoperate with the objective of solving problems, provide functionality or optimize tasks. Topics of interest include (but are not limited to):

- Smart things network and communication: architectures, services and protocols.
- Smart things: privacy, security and identification.
- Internet of Things systems and applications.
- User-centric solutions to define IoT collaborative process.
- Innovative IoT Solutions for handicapped persons.
- Smart things and RFID/NFC communications.
- Intelligent systems based on connected vehicles.
- Smart things networks for real world data management.
- Practical experiences in Smart cities, large-scale IoT systems.
- Opportunistic IoT, based on opportunistic networking techniques.

Keywords: RFID, IoT, NFC,M2M

I. INTRODUCTION

The Internet of Things (IoT) becomes an attractive research topic, in which the real entity in physical world becomes virtual entity in cyber world, and both physical and digital entities are enhanced with sensing, processing, and self- adapting capabilities to perform interaction through special addressing scheme. Along with the combination of Internet and modern sensor technologies such as Radio Frequency Identification (RFID), Near Field Communication (NFC), and Wireless Sensor and Actuator Networks (WSAN), IoT itself is suffering from more rigorous security challenges. Several issues in terms of system architecture, standard, and human involvement are subsequently raised. The following security problems seem to be intense speculations, such as how to design appropriate security framework for things' intelligent applications? What is advanced security technology applied into mass data processing? How to maintain a balance between things' high security requirements and supporting infrastructures' hardware limitation? And how human society securely participates in both cyber and physical worlds with inter- connection?

Such significant obstacles influence the development of the future IoT, along with the exposure of mass data which causes various potential vulnerabilities from robust adversaries. Besides, resource restrictions including

heterogeneous networks and sensor nodes, communication channels/interfaces, bandwidth, storage, and energy, may also induce unique model design. Towards the general IoT, studies on its architecture model, standard, communication protocol, and network management have been researched. Towards the particular IoT security, there are several open issues such as cryptographic algorithms, authentication protocols, access control, trust/privacy, and governance frameworks. Several researches mainly focus on specific communication techniques (e.g., WLAN, RFID), detailed cryptographic mechanisms (e.g., key management), and practical applications (e.g., supply chain management, multimedia traffic).Meanwhile, the security frameworks in traditional networks can also provide merits for IoT security protection. However, security issue towards the future IoT is not a simple technically tough problem, but a multidimensional topic which combines the information security, network security, infrastructure security, and management security. Most existent schemes provide solutions for special communication techniques or applications, which may lack universality for the complicated system. Thus, we will establish an integrated security architecture to promote universal security consideration for the future IoT. In the paper, we focus on a typical future IoT architecture (short for U2IoT), Protocol, Technologies, Application, Issues, Security, Services which comprises two subsystems that Unit IoT and Ubiquitous IoT. In the U2IoT model, conceptions of mankind neural system and social organization framework are introduced for the future IoT. Thereafter, we propose a systematic security architecture (named IPM) by integrating the awareness and interactivity of cyber world, physical world, and human social into the U2IoT model. Meanwhile, the proposed IPM is presented with embedded interactions among information, physical, and management. Specifically, 1) information security model with the considerations for basic and advanced security requirements that are mapped into the security layer to deal with sensing, networking, application, and social attribution; 2) physical

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

security including external con-text and inherent infrastructure are inspired by artificial immune, and it ensures that the things should be adapt-able to dynamic semantic contexts with innate and adaptive immunities against malicious attacks; 3) management security provides recommended strategies for hierarchical classified scenes with rationality and compatibility. IPM realizes the unison of cyber world, physical world and human social to guarantee security and privacy for U2IoT.

The remainder of the paper is organized as follows. In Section 2, we illustrate the existent U2IoT model, and pro-pose the security architecture (IPM). The main features of IPM referring to information security, physical security, and management security are given in Section 3. Finally, Section 4 draws a conclusion.

The Internet can be described as a ubiquitous infrastructure that has evolved from being a technology for connecting people and places to a technology connecting things. The future is the Internet of Things (IoT), which aims to unify everything in our world under a common infrastructure, giving us not only control of the things around us, but also keeping us informed of the state of the things around us. One of the main problems with IoT is that it is so vast and such a broad concept that there is no proposed, uniform architecture. In order for the idea of IoT to work, it must consist of an assortment of sensor, network, communications and computing technologies, amongst others. But when you start putting together different types of technologies, the problem of interoperability arises. One proposed solution is to adopt the standards of the services-oriented architecture (SOA) deployed in business software systems. Another takes a similar approach, suggesting the integration of Web Services into sensor network with the use of IoT optimized gateways, which would bridge the gap between the network and the terminal. In general, it may be beneficial to incorporate a number of the technologies of IoT with the use of ser-vices that can act as the bridge between each of these technologies and the applications that developers wish to implement in IoT. This paper breaks down four main categories of services according to technical features, as proposed and described by [3]. In categorizing IoT services, we aim to provide application developers a starting point, giving them something to build upon so that they know the types of services that are available. This will allow them to focus more on the application instead of designing the services and architectures required to sup-port their IoT application. The IoT envisions hundreds or thousands of end-devices with sensing, actuating, processing and communication capabilities able to be connected to the Internet. These devices can be directly connected using cellular technologies such as 2G/3G/Long Term Evolution and beyond (5G) or they can be connected through a gateway, forming a local area network, to get connection to the Internet. The latter is the case where the end-devices usually form Machine to Machine (M2M) networks using various radio technologies, such as Zigbee (based on the IEEE 802.15.4 Standard), Wi-Fi (based on the IEEE 802.11 Standard), 6LowPAN over Zigbee (IPv6 over Low Power Personal Area Networks), or Bluetooth (based on the IEEE 802.15.1).Regardless the specific wireless technology used to deploy the M2M network, all the end-devices should make their data available to the Internet. This can be achieved either by sending the information to a proprietary web server accessible from the Internet or by employing the cloud. Online platforms such as "ThingSpeak.com" or Open.Sense, among any other alternatives, are virtual clouds able to receive, store, and process data. Besides acting as remote data bases, M2M clouds also offer the following key services:

1. They offer Application Programming Interfaces (API) with built-in functions for end-users, thus providing the option to monitor and control end-devices remotely
from a client device.

2. They act as asynchronous intermediate nodes between the end-devices and final applications running on devices such as smart phones, tablets or desktops. Our paper focuses on the protocols that handle the communication between the gateways, the public Internet, and the final applications. They are application layer protocols that are used to update online servers with the latest end-device values but also to carry commands from applications to the end-device actuators.

The rest of the paper is organized as follows. Section 2 describes our research motivation whereas each of the other sections is dedicated to a specific application layer protocol. At the first part of each section we introduce each application layer protocol, we present its usage, we discuss the reliability and security features it offers and we then compare its suitability for the IoT with other application layer protocols. Finally, in Section 9, we present overall conclusions based on the previous sections and we provide further research areas.

2 Research Motivation:
The IoT is a term used for a huge wave of innovation originated in industries, but currently heading to urban centers, in-home environments, and individuals.

II. TECHNOLOGIES INVOLVED

There are several technologies that can be used to implement the concept of Internet of Things. In this section, we discussed the following technologies:

-Radio Frequency Identification (RFID)
- Near Field Communication (NFC)
- Machine-to-Machine Communication (M2M)
-Vehicle-to-Vehicle Communication (V2V)

2.1 Radio frequency identification (RFID):

RFID system is composed of one or more reader(s) and several RFID tags. Tags are characterized by a specific address and are applied to objects. Tags uses radio frequency electromagnetic fields to transfer data attached to an object. The tags contained electronically stored information which can be read by the RFID reader when the object came in the proximity of the reader (WIKIPEDIA, 2013). RFID allows to monitor objects in real-time, without the need of being in line-of-sight. From the physical point of view RFID tag or label is a tiny microchip combined with an antenna in a compact package. The tag's antenna picks up signals from an RFID reader and then returns the signal, usually with some additional information. Hitachi has developed a tag with dimensions 0.4*0.4*0.15 mm (ATZORI; IERA; MORABITO, 2010).The RFID tags comes in three configurations, the first one is Passive Reader Active Tag(PRAT) in which the reader is passive and receives the signal from the battery operated active tags. The transmission range of the RFID tag and the reader is from 1-2000 feet depending upon the architecture. The second one is Active Reader Passive Tag (ARPT), which is most commonly used. This tag does not have onboard power supplies, so it harvests the energy required to send data from the query signal sent by the RFID reader. The last one is an Active Reader Active Tag (ARAT). In this both the

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

reader and the tags are active, but tags are only awoken by the reader when it comes in the proximity of the reader. Transmission may appear in various frequency bands spanning low frequencies (LF) at 124-135 KHz up to ultra-high frequencies (UHF) at 860-960 MHz (WIKIPEDIA, 2013).An Electronic Product Code (EPC) is one common set of data stored in a tag. EPC's are coded on RFID tags because of which objects can be tracked and identified uniquely. The tag contains a 96-bit string of data. The first eight bits are a header which identifies the version of the protocol. The next 28 bits identify the organization that manages the data for this tag, the organization number is assigned by the EPC Global consortium (EPCGLOBAL, 2013). The next 24 bits are an object class, identifying the kind of product; the last 36 bits are a unique serial number for a particular tag. These last two fields are set by the organization that distributed the tag (WIKIPEDIA, 2013). Rather like a URL, the entire electronic product code number can be used as a key into a global database to exclusively identify a particular product (BURLINGTON, 2009). The RFID tags are used in many applications like Monitoring the life cycle of a product, manage the inventory in the warehouse, tracking of goods, tracking of animals, airport baggage tracking logistics (HARRISON, 2009), mobile payment, etc. We can combine the RFID technology with the other technologies like sensing technology to open a new horizon for new applications.

2.2 Near field communication (NFC):

NFC is quite similar to RFID, or it can be looked as an integration of RFID reader into a mobile phone, which makes NFC customer-oriented as mobile phone is the most popular personal device worldwide (VILMOS; MEDAGLIA; MORONI, 2011). NFC can also be seen as a type of radio communication between NFC enabled mobile devices by touching them together or bring close in the proximity of the other phone. From the technical point of view, NFC operates within the unlicensed Radio Frequency band of 13.56 MHz (MEDAGLIA, 2011); the typical operating range of NFC device is 20 cm. The operating range is directly depended on the size of the antenna in the device. NFC is a short range, low power wireless link evolved from RFID that can transfer small amounts of data between two devices held in proximity. Unlike Bluetooth, no paring is required before the actual transfer of data (TECHRADAR, 2013). NFC enabled communication between the smart objects is safe as this cannot be done from a remote location, so one with his/her NFC enabled device should be present there for the application like payment. The NFC technology will significantly contribute to the future development of IoT. It will provide the necessary tool to be wirelessly connected to any smart objects. Mobile NFC also has the potential to transform the mobile headsets into different types of smart objects like when we need to pay the bills and then our mobile can be used as our credit card.

2.3 Machine-to-Machine Communication (M2M)

Machine-to-Machine (M2M) refers to the communications between computers, embedded processors, smart sensors, actuators and mobile devices (DYE, 2008). The use of M2M communication is increasing in the scenario at a fast pace. For instance, researchers predicted that, by 2014, there will be 1.5 billion wirelessly connected devices excluding mobile phones. There are four components of M2M which are sensing, heterogeneous access, information processing, application and services (CHEN; WAN; LI, 2012).From the technical point of view, M2M is a five-part structure (ETSI, 2013) shown in Figure 2. The structure is defined as follows:

M2M Device: A device capable of replying to request for data contained within that device.

M2M Area Network (Device Domain): Provide connectivity between M2M Devices and M2M Gateways.

M2M Gateway: Use M2M capabilities to ensure M2M Devices inter-working and interconnection to the communication network.

M2M Communication Networks (Network Domain): Communications between the M2M Gateway(s) and M2M application.

M2M Applications: Contains the middleware layer where data goes through various application services and is used by the specific business-processing engines.

M2M has several applications in various fields like healthcare, smart robots, cyber transportation systems (CTS), manufacturing systems, smart home technologies, and smart grids (LAWTON, 2004). Example of M2M area network typically includes personal area network technologies, such as Ultra-wideband and Bluetooth or local networks.

2.4 Vehicle-to-vehicle (V2V) communication:

V2V Communication is a new concept in which lots of research has to be done. In this, vehicles act as a node in a network and communicate with each other with the use of sensors connected in an ad-hoc network. The infrastructure of V2V network is a bit complicated as there is no fixed topology to be followed as vehicles are moving from one place to another all the time. Applications for vehicular networks can be divided into four broad categories, namely safety and collision avoidance, traffic infrastructure management, vehicle telematics, and entertainment services and Internet connectivity (BOOYSEN; ZEADALLY; ROOYEN, 2011).Vehicles communicate with each other within a range of 1000 m. Two types of communication are possible; first one is vehicle-to-vehicle and the other one is the vehicle with the road-side infrastructure. Vehicular communication system is developed as a part of Intelligent Transport System (ITS). From a network architecture point of view, focus is initially placed on routing protocols; Physical layer (PHY), Medium Access Control (MAC) layer, and broadcasting (BOOYSEN; ZEADALLY; ROOYEN, 2011).

III.APPLICATION

Ample of application is there where Internet of Things is playing a vital role. In the near future, there will be even more applications using Internet of Things. As the world is going through a technological revolution, more and more objects will use the technology of RFID,NFC, M2M communication and V2V communication for automation as shown in Figure 3.

3.1 Transportation and logistic domain

3.1.1 Smart parking:

The new Smart Parking sensor's to be buried in parking spaces to detect the arrival and departure of vehicles. The Smart parking provides extensive parking management solutions which helps

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

motorists save time and fuel (LIBELIUM, 2013). A significant contribution to congestion arises from motorists searching for accessible parking spaces. Providing accurate information about parking spaces helps traffic flow better, and this will also allow the deployment of application to book parking spaces directly from the vehicle. This will help to reduce CO_2 emissions and to minimize traffic jams.

3.1.2 3D Assisted driving:

Vehicles like cars, buses and trains along with the roads and rails equipped with sensors may provide valuable information to the driver to provide better navigation and safety. With the use of assisted driving, we will be able to find the right track with prior information about traffic jams and incidents. In an Enterprise context, information about the vehicle transporting goods together with information about the type and status of the goods can integrate to provide valuable information about the delivery time, delivery delays and faults.

3.1.3 Augmented maps:

Tourist augmented maps with tags allow NFC-equipped phones to browse the information about the places and quickly connect it to the web services providing information about hotels, restaurants, monuments, theatre and the local attractions. This can be done by hovering your mobile phone over the tag within its reading range so that the additional information about the marker can be displayed on the screen.

Logistics:

Implementing the Internet of Things in Retail chain monitoring has many advantages: RFID and NFC can be used to monitor almost every link of supply chain, ranging from commodity details, raw material purchasing, production, transportation, storage, sale of product and after sales services. With the help of IoT, we will track the inventory in the warehouse so that stock can be refilled at the appropriate time for continuous sale and this will reduce the waiting time of customer which result in customer satisfaction, which further results in increased sales.

3.2 Healthcare domain

3.2.1 Health tracking:

We can track health of a person with the help of combination of RFID and NFC technology together. With the use of sensors and the technology stated above we can track the person's body temperature, heart beat rate, blood pressure, etc. In case of emergency, the individual and their personal doctor will be notified with all the data collected by the sensors.

3.2.2 Pharmaceutical products:

Safety of pharmaceutical product is of utmost importance to prevent the health of patients. Attaching smart labels to drugs, tracking them through the supply chain and monitoring their status with sensors has benefits like items require specific storing conditions so they can be monitored whether their requirements are fulfilled or not. We can also track the expiry of drugs with the use of sensors; this will prevent the transferring of expired drugs to the patient.

3.2.3 Data collection:

Automatic data collection and transfer of that data to the doctor will help in reducing in the processing time, reducing the data collection errors, automated care and routine auditing. This will also forward all the previous health record related to the patient which helps in accuracy of the medication given by the doctor.

3.3 Smart environments domain

3.3.1 Smart water supply

Smart cities must monitor water supply to ensure that there is adequate access for resident and business need. Wireless Sensor Networks provide the technology for cities to monitor their water piping systems more accurately and discover their greatest water loss risks. Cities that are addressing water leakage problem with sensor technology are producing high savings from their investment. Tokyo, for example, has calculated they save $170 million each year by detecting water leakage problems early (LIBELIUM, 2013). The system can report pipe flow measurement data regularly, as well as send automatic alerts if water use is outside of an estimated normal range. This allows a smart city to determine the location of leaking pipes and prioritize repairs based on the amount of water loss that could be prevented.

3.3.2 Smart homes and offices:

We are surrounded by various electronic gadgets around us such as microwave ovens, refrigerators, heaters, air conditioners, fan and lights. Actuators and sensors can be installed in these devices in order to utilize the energy sufficiently and also to add more comfort in life. These sensors can measure the outside temperature and even can determine the occupants inside the rooms and thereby control the amount of heating, cooling and flow of light etc. Doing all these can help us to minimize the cost and increase energy saving.

3.3.3 Improved gyms:

The gymnasium experience can be enhanced by involving new technologies like a separate exercise profile which can be installed on machines and each person can be identified from his identification id alone and thereby, concerned profile will get activated.

3.3.4 Food sustainability:

Food that we eat has to go through various stages before they arrive in the refrigerators. They are bound in a strict food cycle: production, harvesting, transportation and distribution. With the use of appropriate sensors, we can prevent the food from climatic damages by keeping a good eye on temperature, humidity, light, health etc. Sensors can measure these variations precisely and notify the concerned person. Monitoring helps in prevention of possible plant.

3.4 M2M and V2V communication domain

3.4.1 Industrial Maintenance:

The sensors fit in the machinery are used to monitor the temperature and vibration in industrial motors, and also warn when irregular operation is detected. Industrial maintenance is the term for the task of keeping the equipment running at peak

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

efficiency in a factory. It includes scheduled cleaning, parts replacement and lubrication and repairs. The field of industrial maintenance does not involve just the repair of already existing malfunctions (LIBELIUM, 2013), but preventive maintenance typically is also a vital part of the field. Companies waste billions due to inefficient maintenance management. This will help Companies to save money and time.

3.4.2 Smart Cars:

Machine to machine (M2M) communications, and especially Smart Cars, could help to improve accident prevention. A pilot to operate remote control car in order to minimize car accident and reduce human error was developed by McGill University (SANTORELLI; MORAWSKI;LE-NGOC, 2011). These driverless cars will provide functioning more than just safety such as they can save valuable time, reduce stress of driving etc. Some studies carried out by the Institute of Electrical and Electronics Engineers (IEEE) reveal that, by 2040, driverless cars will account for up to 75 per cent of cars on the road worldwide (LIBELIUM, 2013).

3.4.3 Smart Grid:

Smart Grid is defined as an electrical grid which is designed to improve the efficiency of power transmission, and quality of service to the end user. In Smart Grid, all the devices in the network are connected with the sensors which regularly send the data related to power consumption to the central server. Central server determines the pattern of consumption and the amount of power consumption. This allows companies to increase their production to meet the transient power requirement (BOOYSEN et al., 2012).

3.5 NFC application domain

3.5.1 Travelling:

NFC can enhance the travelling experience to a greater extent: it can help us to minimize the check in time during the stay in hotels. When the room is booked in a hotel, a secure digital key is sent to the traveller. One can use that digital ticket, with the NFC enabled locks, and directly enter into the room without wasting any time in check-in lounges.

3.5.2 Health:

NFC can be useful in monitoring personal health. It can gather information about health and send the collective data to health monitoring center. These centers can, therefore, analyse health and provide the valuable report and information to the individual.

3.5.3 Payment:

With the help of NFC technology, a user can leave his credit cards at home and can make a copy of credit cards on the mobile device. In case he needs to make any payment, he can electronically make the payment by using the clone of credit cards on the mobile phone, and NFC activated devices.

In scenario, the effect of IoT can be seen in all technical areas. It helps in smart communication between objects but several issues are there to be addressed before the worldwide implementation of IoT. In this section, we identify some important issues related to addressing, routing protocol, security and privacy, standardization issue and congestion and overload issue.

3.5.4 Addressing and networking issue:

Each and every device connected in the network has a unique address by which it can be identified. As the IoT is gaining grounds in scenario, the demand for these unique address increases at a very fast rate. There are very limited number of address available in IPv4 addressing and will soon reach zero as it identifies each node through a 4-byte address. To handle the ever increasing demand of unique address, one require IPv6 addressing scheme to fulfil the requirement. IPv6 addresses are expressed by means of 128 bits and, therefore, it is possible to define 1038 addresses, which should be enough to identify any object. Another important issue is regarding networking i.e. which protocol is to be used to send the data from source to destination. In traditional internet, the protocol utilized at the transport layer for reliable communications is the Transmission Control Protocol (TCP) (CERF;DALAL; SUNSHINE, 1974). It is clear that TCP is insufficient for the IoT because we need to set-up a connection first in case of TCP, but most of communication in IoT is a very short communication. So, considerable time will be wasted in the connection setup. One more issue with TCP is congestion control, TCP is responsible for end-to-end congestion control, but in case of IoT the amount of data transfer is very small, so TCP congestion control is useless. As a consequence, TCP cannot be used efficiently for the end-to-end transmission control in the IoT. Till now, no solutions have been proposed and, therefore, research is required in this area.

3.5.5 Routing protocol issue in V2V communication:

Routing is a very important aspect in the field of V2V communication as it is a type of distributed processing with a great number of nodes and a constrained and highly variable network topology. There are two basic ways by which one can route the data from source to destination. The first one is source routing: in this all the information like how to get from source to destination is collected on the source and then stored in the packets to be send, and the job of the intermediate node is to read this information and route the packet according to it towards the destination. Second one is hop-to-hop routing: in this routing technique, node has information only about the next node; the work of intermediate node is a bit complex as they know the destination address only, not the whole route to get towards the destination (KUMAR;KUMAR; KADIAN, 2011). This hop-to-hop is more efficient as in this we can choose the best next hop according to the topology. The architecture of routing in V2V communication is the same as the architecture of routing in other connectionless networks. Routing is the backbone of the network. There are lots of protocols present there like Geographical Source Routing (JERBI et al., 2009) which is hop-to-hop routing. This routing is based on the topology information given by global positioning system; frequently changes in topology causes route oscillation and path instability. In On-Demand Routing protocol (DAS; PERKINS; ROYER, 2000) node attempts to discover a route to the destination when it has a packet to send. In this protocol, flooding method is used to discover the route which creates the congestion in the network as it sends the packet to all the nodes for route discovery. There are various other routing technique like Greedy Perimeter Stateless Routing (GPSR)(KARP; KUNG, 2000), Dynamic MANET on Demand (DYMO) (CHAKERES; PERKINS, 2006),etc., but each one has its shortcoming. The key challenge is to design a protocol which will improve reliability of protocols and reduce

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

delivery delay time and number of packet transmission. To make VANET a reality, lots of research is needed as each one of the existing protocol has some drawbacks as explained above. The driver behaviour should also be concerned in designing the routing protocols.

3.5.6 Privacy and security issue:

The IoT is extremely vulnerable to attacks as its components spend most of the time unattended, so it became very easy to attack them. Apart from this, one more thing is that, most of the communication is wireless which makes snooping very easy. This is probably one of the biggest concerns for consumers when it comes to IoT. For instance, in NFC enabled devices, the device not only works as a credit card but also the key to your house, it will also contain the personal information of the owner. If a smartphone is stolen, the thief move's the phone over a card reader at a store to make a purchase (NFC, 2013). To avoid this, smartphone owners must protect their phone with strict password protection, so hacker is not able to come out with the correct password. More specifically, the major problems related to security concern authentication and data integrity. Authentication is required before making a connection between the two devices to prevent data theft. The infrastructure is required for the authentication as we generally have to exchange some public and private keys through the node. Solutions like cryptography and key management have been proposed in the recent past (e.g., (KAVITHA; SRIDHARAN, 2010),(ESCHENAUER; GLIGOR, 2002a)), but none of them will prevent from the man-in-the-middle attack and proxy attack problem.

Data integrity prevents any modification in the data by middle man; it ensures that the data received at the receiver node is in the unaltered form as send by the sender. Solutions have been proposed like Keyed-Hash Message Authentication Code (HMAC) scheme (ESCHENAUER;GLIGOR, 2002b), to protect the data against the attack but still new research is required in the field of security and privacy.

3.6 Standardization issue:

Standards are required to allow global interoperability. As the term Internet of Things is gaining popularity, the more and more number of devices is activated daily. To ensure the proper functionality of these devices, there should be certain standards we have to follow to provide proper service to the client. As the platform on which these IoT devices works is not the same in all cases, so it became more necessary to define certain standards to make those devices compatible with the others. EPCglobal (Electronic Product Code) (EPCGLOBAL, 2013),as well as ISO (International Organization for Standardization), offers a family of standards, and they are gaining popularity in the wireless sensor area.

3.7 Congestion and overload issue:

Congestion is occurred due to simultaneous messages from several devices that can lead to peak load situation and may have a tremendous impact on the network (3GPP, 2010). This affects the performance of the network, and may lead to failure of the network if the network is overloaded. This situation is mainly seen in M2M and V2V communication, and it can be solved with the help of emerging technologies like LTE-advanced or existing technologies like LTE high bandwidth networks (TALEB; KUNZ, 2012). The congestion situation also occurred because of malfunction of server or application; so to avoid this one has to design an application in such a way that can handle maximum load with minimum failure. Overload issue can be solved with the help of time controlled features, i.e., allow connection to the network only at a certain time periods, defined by the network operator. Only in this time period, the devices are allowed to connect, devices are not able to connect to the network in the forbidden time period. The other solution is by rejecting the connection request by specific network nodes, particularly from those that are causing congestion and shall have no impact on the traffic (TALEB; KUNZ, 2012). This will help in managing the overall load of the network by rejecting the nodes which are creating the congestion.

IV ARCHITECTURE

4.1 Proposed Security Architecture for U2IoT:

The U2IoT model is shown in Figure 1(a), which is essentially a heterogeneous system including Unit IoT and Ubiquitous IoT. Thereinto, Unit IoT resembling human neural network, refers to the basic cell providing solutions for special applications. Ubiquitous IoT includes the industrial IoT, local IoT, national IoT, and global IoT which is integration of multiple Unit IoTs with ubiquitous features, and it is similar to the social organization framework.

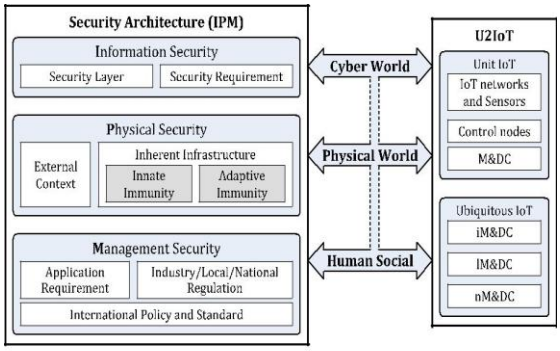

FIGURE 1. U2IOT MODEL AND ITS SECURITY ARCHITECTURE (IPM). (A) THE U2IOT (UNIT IOT AND UBIQUITOUS IOT) MODEL; (B) THE PROPOSED SECURITY ARCHITECTURE (IPM) BASED ON U2IOT.

I: Information security includes two perspectives (*i.e*., security layer and security requirement). Awareness of information data is captured, interpreted, and rep-resented by things' capability, along with aggregation algorithms, protocols, and functions are included for intelligent information interactions.

P: Physical security relates to environmental monitoring, motion detection, localization, tracking, perimeter control, and consumption supervision. The concept of artificial immunity is applied to detect passive and active defenses for maintaining homeostasis.

M: Management security provides the recommended application requirement, industry/local/national regulation, and international policy and standard to guide activities and events in the human social. In IPM, human social activities occurring in physical world are identified and mapped into the unique cyber world, which realizes harmonious unification of human, network and things. Such triple relationships of entity in U2IoT, makes entity identification and service discovery are effectively

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

performed in current cyber-physical world, and are easily to extend to human social and its social networks. The security aspects underline main characteristics of U2IoT entities.

4.2 Information Security

Information security protects both raw data and contextualized information, and an information security model that comprises U2IoT, security layer, and security requirement is established in **Figure 2**.

1) *Considering Social Factor for Security Layer*: U2IoT is generally divided into four layers as follows.

Sensor layer: it comprises generalized sensors and gateways to perform entity identification and service discovery. The function of sensor layer is to perceive the entities, to extract information, and to realize se-mantic resource discovery. The sensor techniques are applied to realize effective integration and interaction adaptation of the collected uncertain information.

Network layer: it includes network interfaces, communication channels, network management, information maintenance, and intelligent processing. The centralized, distributed, and hybrid network topologies are involved to assist monitoring and maintaining the real-time network configuration. The network layer ensures reliable information transmission by adopting data coding, extraction, fusion, restructuring, mining, and aggregation algorithms. The main function is to transfer and process the information obtained by sensor layer, and to realize data exchange among large-scale heterogeneous networks.

Application layer: it exports functionalities for specific applications, and provides embedded interfaces for infrastructures to perform testing, monitoring, or auditing applications. The standard protocols and service composition technologies are applied to realize the integration between heterogeneous distributed networks and its applications, such as logistics monitoring, smart grid scheduling, intelligent search, and cloud computing. Such applications should adapt in dynamic environments.

Particularly, an additional social layer on the top of the architecture considers the social attribution in U2IoT. The social layer is mainly devoted to communicate among objects and other supporting networks to perform correlation between the cyber individual and the corresponding profile in social networks. Correlative social attributions are granted to each entity, and hierarchical management and data centers operate overall security considerations. In social layer, diverse interfaces are accessed by a real entity which acts on its corresponding cyber entity to control its behaviors. Meanwhile, other social compositions are also considered, such as ownership control management, social relationship modeling, and entity behavior formalization. In the perspective of information security, the sensor and network layers specify multiple networks and sensor nodes, which are used to capture data streams, to detect activities and events with identification algorithms, and to realize specific application functions. Core of data acquiring is sensor technology (e.g., RFID, WSN, femtocell) and Global Sensor Network (GSN) middleware, whose security is challenged by constrained resources. Note that distributed control nodes provide the capabilities to survive under formidable conditions, and by information security controls such as error detection and correction, random access control, and fault tolerance are recommended.

2) *Adding Intelligence and Compatibility for Security Requirement*: Elements of security requirements include CIA Triad, authority, non-repudiation, and privacy. Additional requirements that intelligence and compatibility are added into advanced security considerations, which provide reliable security and privacy protection. **Table 2** presents the comparison of security requirements among the traditional network, general IoT, and U2IoT. *Intelligence* represents that an entity should own abstract capabilities including self-learning, self- *Compatibility* requires that an entity has appropriate interconnection and interoperability to adjust to heterogeneous data formats, interfaces, channels, and networks in U2IoT model. The supplemental requirements address advanced criterions for information interaction. Meanwhile, compatibility can be promoted to scalability, expansibility and modularity among heterogeneous entities and the multi-context environments.

The both requirements operate together to promote the security and privacy preservation: 1) ensure diverse entities own artificial intelligence and autonomous security control against the strong attackers; 2) ensure heterogeneous entities, networks and applications establishing re-liable interconnection without compromising any communication data and individual privacy.

Physical security is denoted in external context and inherent infrastructure, in which human-like security immune safeguard is achieved.

1) *External Context*: Simple context and complex con-text are specified in [16], in which the former determines the basic identity, location, and entity status by a single parameter; the latter refers to geographical structures, traceability information, and real world conditions. Above both contexts are refined to support creating, debugging and integrating applications of Ubiquitous IoT, and provide interface interconnection and restriction for Unit IoTs. In U2IoT model, the borders of each entity's external con-text merge even vanish, and the obscure contexts spanning from an individual, an object, or an environment to social relationships, should support the hierarchical IoT subsystem. Particularly, intrusion detection algorithm is significant to acquire context information for monitoring sensors behavior, discover control node breaches, and other potential vulnerabilities.

2) *Inherent Infrastructure*: Artificial immune security system as computational intelligence is applied to analyze inherent infrastructure, which belongs sensorial sys-tem inspired by principles and processes of the natural immune system. Typical algorithms (e.g., clonal selection, negative selection, and immune network) exploit the immune system's features of detection, learning and memory to constitute innate immunity and adaptive immunity. Physical security issues such as intrusion detection, adaptive disposition, context-driven feedback, and error recovery can be addressed as follows.

3) Innate immunity: It provides basic barriers against foreign invasions in real-time environment, and it is triggered upon sensors identifying abnormal or malevolent attacks by the intelligent pattern recognition mechanisms. Co-stimulation signals are transmitted to distributed control nodes via Unit IoT networks, and then rejection reactions are performed by management centers. During defense operations, activation thresh-olds are defined to ensure the detection optimization, and fuzzy diagnosis can also applied for imperfect detection. Note that the innate immune defense is non-specific, meaning that U2IoT model responds to the various attacks in a general scheme. Such system can-not afford long-lasting immunity

DOI 10.17148/IJARCCE.2017.6326

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

against a certain at-tack. The innate immune system is dominant to con-front the dynamic contexts and continuously refreshing threats.

4) Adaptive immunity: It refers to acquired resistance, where an attack is marked as a specific signature. Selective response requires recognizing non-self element during attack prototype presentation. If U2IoT has been infected by the same or similar invasion, specific memory module would be aroused to eliminate damaging effects by generating improved response to return the system into secure state. Adaptive immunity executes fuzzy diagnosis to variations of the same former attack, and optimal stimulation such as subsidiary vaccination is available by updating M&DCs' profile databases. According to both innate and adaptive immunities, three main features should be achieved in U2IoT model.

***5. Multithreaded and Hybrid Configuration*:** The U2IoT model may apply multithreaded security algorithms for the massively parallel network architecture that comprises a diverse set of components. The components are organized in hybrid mode, in which both centralized and distributed configurations are included. Towards Unit IoT, the allocation of the sensing and query processing is performed by the central M&DC. Towards Ubiquitous IoT, the industry IoTs and local IoTs are relatively independent, which commonly construct national IoT. In U2IoT model, such multithreaded and hybrid configuration are through-out all the networks, sensor and control nodes, and management and data centers.

***6. Multilayered and Autonomous Organization*:** There is no single security mechanism that offers complete immunity. Therefore, multilayered protection should independently operate for all-round safeguards. During the layered organization, U2IoT model autonomously makes its decisions by detecting potential attacks and proposing feasible solutions based on artificial immune algorithms.

***7. Heterogeneity*:** U2IoT model should be accessible by a large number of heterogeneous communication technologies with different networks, channels, interfaces, and hard-ware/software capabilities. Such heterogeneity of entities adds complexity to its security situations, which makes that a certain attack may simultaneously act on multiple entities in different IoTs, but the attack cannot act on all the involved IoTs. The immune protection ensures that the entire heterogeneous components cannot be corrupted due to the same attacker.

4.3. Management Security

Towards the future IoT, it is scarcely possible to establish a uniform security protocol as Internet, just like different nations and/or regions cannot adopt an identical safety precaution. Hence, distinctive management mechanisms are significant for both security and interconnection requirements. Due to the limitations of technological approaches, appropriate management should couple with the implementation of information security and physical security. Security strategies working on human behaviors should be considered to ensure that virtual cyber data is adapted to the real physical contexts.

4.3.1Application requirement for distributed sensor and control nodes provides generic/specific protection. IPM is of benefit to practical application security, such as historical query, project management, risk assessment, software de-sign, and system certification. For a specific scenario, customized requirements are assigned to describe the authorized/-unauthorized usage in a particular organization or individual. Additionally, application requirement should also be consistent with privacy prevention which realizes that the sensitive data is exchanged, stored, and shared with-out revealing any user privacy.

4.3.2Industry/Local/National regulation mainly serves for iM&DC/lM&DC/nM&DC to provide rules and guidance for U2IoT. It takes legal or disciplinary actions to resist the offensive individuals or institutions which do not com-ply with the regulations. There into, industry regulation describes approaches to achieve high-level security objective for a special industrial authority organization, such as agriculture, energy, and military. For instance, in the chemical hazards medical management, the regulations require certain parameters (e.g., temperature, vibrations, and relative proximity), caution the users for violation thresholds, and guarantee system security by warning abnormal implement and configuration. Thereinto, local regulation should coincide with local customs and practices to adopt humanistic perspectives for designing, implementing, and maintaining the local IoTs. National regulation governs guide-lines to realize nation-to-nation compatibility, and formal memorandum of agreements needs to be shared across national boundaries. Additionally, customized roles and responsibilities can be codified among different nations.

4.3.3International policy: considers the global IoT consociation during connectivity and consistency of nM&DC and global IoT. Moreover, international standards should be addressed by governments to promote security confidence and ensure interoperability. It indicates that a general international governance framework with reasonable enforcement policies will provide permanent mechanism towards security protection.

V.SERVICES

5.1 Types of Services:

There are an exceptional number of applications that can make use of the Internet of Things, from home and office automation to production line and retail product tracking. The number of applications is endless. For each application, a particular IoT service can be applied in order to optimize application development and speed up application implementation. Note that the categorizations that follow come from.

5.1.1 Identity-Related Services

Identity-related services can be divided into two categories, active and passive, and can serve either individuals or enterprise, which can lead to a number of different kinds of applications. The general identity-related service consists of two major components: 1) the things, all of which are equipped with some kind of identification identifier, such as an RFID tag; and 2) the read device(s), which read the identity of the thing based on its label, in this case reading the information encoded into the RFID tag.

5.2 Information Aggregation Services

Information aggregation services refer to the process of acquiring data from various sensors, processing the data, and transmitting and reporting that data via IoT to the application. These types of services can be thought of, more or less, as one way: information is collected and sent via the network to the application for processing.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Information aggregation services do not have to implement a single type of communication channel in order to work together. With the use of access gateways (**Figure 1**), an information aggregation service could make use of different types of sensors and network devices and share their data via a common service to the application. For example, an application could make use of RFID tags to be aware of the identity of some devices, while also using a ZigBee network to collect data from sensors, then use a gateway device to relay this information to the application under the same service, say a Web Service such as JSON or XML. Not only would this allow a developer of an application to incorporate a number of different technologies into the application, but it could also allow the application to access various IT and enterprise services that may already be in place.

5.3. Collaborative-Aware Services

Collaborative aware services are services that use aggregated data to make decisions, and based on those decisions perform an action. As IoT takes shape, it should bring about the development of complicated services that make use of all of the data that can be retrieved from the extensive network of sensors. This will require not only being able to retrieve information, but to relay back responses to the collected information to perform actions. These services will thus require "terminal-to-terminal" as well as "terminal-to-person" communication. By providing collaborative aware services, the IoT infrastructure naturally requires greater reliability and speed, and will require the terminals to either have more processing power or be linked with some other device that does.

5.4. Ubiquitous Services

Ubiquitous services are the epitome of the Internet of Things. A ubiquitous service would not only be a collaborative aware service, but it would be a collaborative aware service for everyone, everything, at all times. In order for IoT to reach the level of providing ubiquitous services, it would have to overcome the barrier of protocol distinctions amongst technologies and unify every aspect of the network. There is no particular system architecture for the Internet of Things, but there have been numerous papers written about the use of Web Services or REST (representational state transfer) APIs (application programming interfaces) to unite loosely coupled things on the Internet under a single application so that they can be reused and shared. IPv6 is also a protocol that could greatly benefit the increase in ubiquitous services. Reference [4] proposes such an architecture that, if implemented, would be considered a ubiquitous service.

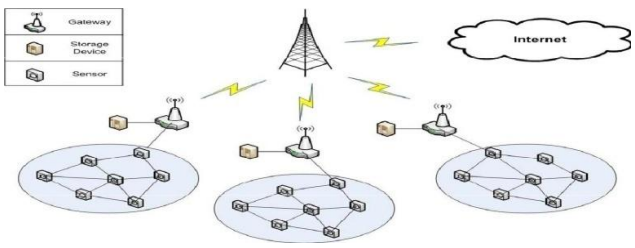

FIGURE 2. RFID NETWORK EXAMPLE.

Moving past what each of the categories means, the following subsections provide examples of each type of ser-vice in an attempt to offer developers a starting point when developing their own application. The idea is to provide a series of examples for each service type that use a common technology so as to provide a basic frame-work to build an application upon a specific type of ser-vice.

V. APPLICATIONS OF IOT SERVICES

6.1. Identity-Related Services

Identity-related services are the most simple, yet maybe one of the most important, services to be provided to an application of the Internet of Things. Applying an identity-related service to an application provides the developer with vital information about every device, or every*thing*, in their application.

The most prominent technology used in identity-related services is RFID. RFID is a technology that enables data to be transmitted by a tiny portable device, called a tag, which is read by an RFID reader and is processed ac-cording to the needs of that particular application. RFID provides an upgrade from the traditional form of device identification: barcode scanning. RFID is more versatile because it does not require line of sight transmission, and, in the case of active RFID tags, can transmit its data as opposed to simply just being read by a reader device.

Most IoT applications that are aimed at providing an identity-related service make use of RFID technology. As described, the RFID tag stores an identification code unique to that device. The RFID reader reads that code, and looks up the device in the RFID server, which then returns the detail information require by the application.

Production and shipping are two common applications that would benefit greatly from the use of an identity ser-vice. Another application that uses an identity-related service describes a model that can solve the information asymmetry problem in supply chain management and supply chain information transmission. Every IoT application will either be based on, or at least incorporate some instance of, an identity-related service. This is because for the IoT to incorporate every-thing in the physical world to the digital world, the application will need to be able to identify all of the devices that are connected.

6.2. Information Aggregation Services

Information aggregation services incorporate identity related services, along with other components such as WSNs, and access gateways to collect information and forward it to the application for processing. The information aggregation service is just responsible for providing the application with all of the information that is collected, and potentially processed along the way, from the terminals of the system (sensors, RFID tags, etc.). In this regard, the WSN can be a powerful tool for collecting and communicating data between terminals and the platform (host of application), as long as the platform is within range of the WSN. But this would not be an IoT application on its own; an IoT application would consist of multiple WSNs all configured to work together to provide information about the world around them. The link between these networks is an access gateway. The general structure of this network is shown in **Figure 2**. Each access gateway in the IoT network will have access to the database server, thus every device would be connected and information from the entire network aggregated at the database server. There are a number of applications out there that make use of information aggregation services and access gate-ways. In [7], the importance of extending the information aggregation service to beyond the WSN is proposed by using a cellular network (CN) to extend the range of the WSN. The idea is that if a terminal is outside of the WSN of interest, it uses CN resources

to access that information through the use of an "IoT gateway," which essentially implements both WSN and CN resources.

Information aggregation services are useful in monitoring situations, such as energy monitoring in the house and in the enterprise, or, if the Internet of Things has been realized, monitoring of anything, anywhere. For example, introduces a monitoring and control system for use in an agriculture greenhouse production environment. The system measures and records critical temperature, humidity and soil signals which is then trans-mitted through the network to the platform for processing. Another application uses a ZigBee WSN to monitor physiological data of patients that automatically generates electronic medical records.

6.3. Collaborative-Aware Services

The key difference between information aggregation ser-vices and collaborative-aware services are the use of the data collected to make decisions and perform actions. As mentioned before, the keys to creating a collaborative-aware service are network security, speed, and terminal processing power. Terminals can no longer be just simple sensors that collect information, or if there are simple sensors in the network, there must be separate embedded devices within the network that can make use of the data.

There are fewer applications published in terms of IoT and collaborative-aware services. We can, however, at-tempt to apply new technologies to a collaborative-aware service. An example of a new technology that will help shape the way the Internet of Things grows is IPv6. IPv6 is a new version of the Internet Protocol (IP) that allows for a significantly greater number of addressable devices to be connected to the internet. Although the use of IPv6 has had a slow start, it is definitely the internet protocol of the future due to the lack of available IP addresses. Moving forward, one of the most important factors in IoT be-coming reality is being able to address each of the embedded devices in the world, which converting to IPv6 would allow. Reference offers a number of applications for IoT, many of which could be considered collaborative-aware services, or which could at least provide a baseline for such a service. They propose integrating every object into the IP infrastructure using both IPv6 and 6LoWPAN, which is the use of IPv6 over low power wireless personal area networks. They propose a network with three types of nodes, all of which can be reprogrammed to function as any of the three types. The three types essentially are a base station node (IPv6 router), a mobile node (wireless dongle that allows WSN connectivity to a standard laptop) and specialized nodes, which are used for specialized tasks. This becomes a collaborative-aware service because it incorporates terminal-terminal and terminal-person communication, which is accomplished due to the use of the IPv6 protocol.

6.4. Ubiquitous Services

Ubiquitous services are the ultimate goal of the Internet of Things, taking collaborative-aware services to the next level by providing complete access and control of every-thing around us, whether it is through a computer or a mobile phone or something else. Ubiquitous services have yet to be realized in the world today, but most research in IoT is ultimately aimed at providing some piece to the puzzle that will ultimately be ubiquitous services. Reference first talks about why the Internet of Things is so difficult to realize. One of the biggest hurdles for IoT is having a single architecture that allows the many different application layer standards to communicate and interoperate. Reference proposes an architecture, based on RESTful services, in which a universal API would be created so that everyone who creates devices to be used in the Internet of Things has an architecture to adopt in order to be interoperable with the rest of the world's devices

REFERENCES

[1] Tasos Kaukalias and Periklis Chatzimisios, Internet of Things (IoT) C Enabling technologies, applications and open issues, Encyclopaedia of Information Science and Technology(3rd Ed.), IGI Global Press, 2014.
[2] Periklis Chatzimisios, Industry Forum & Exhibition Panel on Internet of Humans and Machines, IEEE Global Communications Conference (Globecom 2013), Atlanta, USA, December 2013.
[3] Angelo P. Castellani, Mattia Gheda, Nicola Bui, Michele Rossi, Michele Zorzi, Web Services for the Internet of Things through CoAP and EXI, IEEE International Conference on Communications Workshops (ICC), 5-9 June 2011, pp. 1-6.
[4] Sye Loong Keoh, Sandeep S. Kumar, Hannes Tschofenig, Securing the Internet of Things: A Standardization Perspective, Internet of Things Journal IEEE (Volume:1,Issue: 3), June 2014, pp. 265-275.
[5] Maria Rita Palattella, Nicola Accettura, Xavier Vilajosana, Thomas Watteyne, Luigi Alfredo Grieco, Gennaro Boggia, Mischa Dohler, Standardized Protocol Stack for the 8Internet of (Important) Things, Communications Surveys & Tutorials IEEE 15(3),2013, pp. 1389-1406.
[6] Thamer A. Alghamdi, Aboubaker Lasebae, Mahdi Aiash, Security Analysis of the Constrained Application Protocol in the Internet of Things, Second International Conference on Future Generation Communication Technology (FGCT), 12-14 Nov.2013, pp. 163-168.
[7] Shahid Raza, Hossein Shafagh, Kasun Hewage, Ren Hummen, Thiemo Voigt, Lithe: Lightweight Secure CoAP for the Internet of Things, Sensors Journal, IEEE 13(10),Oct. 2013, pp. 3711-3720.
[8] Shinho Lee, Hyeonwoo Kim, Dong-kweon Hong, Hongtaek Ju, Correlation Analysis of MQTT Loss and Delay According to QoS Level, International Conference on Information Networking (ICOIN), 28-30 Jan. 2013, pp. 714-717.
[9]http://mqtt.org/2011/08/mqtt-used-by-facebook-messenger, cited 28 Jul 2014.
[10] Dinesh Thangavel, Xiaoping Ma, Alvin Valera, Hwee-Xian Tan, Colin Keng-Yan Tan, Performance Evaluation of MQTT and CoAP via a Common Middleware, IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 21-24 April 2014, pp. 1-6.
[11] http://www.zdnet.com/google-moves-away-from-the-xmpp-open messagingstandard-7000015918/, cited 28 Jul 2014.
[12] Sven Bendel, Thomas Pringer, Daniel Schuster, Alexander Schill, Ralf Ackermann, Michael Ameling, A Service Infrastructure for the Internet of Things based on XMPP,IEEE International Conference on Pervasive Computing and Communications Workshops(PERCOM Workshops), 18-22 March 2013, pp. 385-388.
[13] Michael Kirsche, Ronny Klauck, Unify to Bridge Gaps: Bringing XMPP into the Internet of Things, IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), 19-23 March 2012, pp. 455-458.
[14] Roy Thomas Fielding, Architectural Styles and the Design of Network-based Software Architectures, PhD thesis, University of California, Irvine, USA, 2000.
[15] Bipin Upadhyaya, Ying Zou, Hua Xiao, Joanna Ng, Alex Lau, Migration of SOAP based Services to RESTful Services, 13th IEEE International Symposium on Web Systems Evolution (WSE), 30 Sept. 2011, pp. 105-114.
[16] http://en.wikipedia.org/wiki/Advanced Message Queuing Protocol, cited 28 Jul 2014.
[17] Frank T. Johnson, Trude H. Bloebaum, Morten Avlesen, Skage Spjelkavik, Bjørn Vik, Evaluation of Transport Protocols for Web Services, Military Communications and Information Systems Conference (MCC), 7-9 Oct. 2013, pp. 1-6.
[18] Joel L. Fernandes, Ivo C. Lopes, Joel J. P. C. Rodrigues, Sana Ullah, Performance Evaluation of RESTful Web Services and AMQP Protocol, Fifth International Conference on Ubiquitous and Future Networks (ICUFN), 2-5 July 2013, pp. 810-815.9
[19] http://www.amqp.org/about/examples, cited 28 Jul 2014.
[20] http://en.wikipedia.org/wiki/WebSocket, cited 28 Jul 2014.
[21] Victoria Pimentel, Bradford G. Nickerson, Communicating and Displaying Real-Time Data with WebSocket, Internet Computing IEEE 16(4), July-Aug. 2012, pp. 45-53.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

BIOGRAPHIES

MOHD ANWARUDDIN, received B.Tech. Degree in Electronics and Communication Engineering from JSN College of Engineering & Technology, Adilabad and M.Tech. in DECS from JNTUA College of Engineering, Anantapur. He is an Assistant Professor of the Dept. of ECE in Nawab Shah Alam Khan College of Engineering & Technology, Malakpet, Hyderabad.

MOHD ABDUL SATTAR, received B.Tech. Degree in Electronics and Communication Engineering from National Institute of Technology(NIT), Warangal and M.Tech. in Embedded Systems from JNTUH. He is an Associate Professor & Head of the Dept. of ECE in Nawab Shah Alam Khan College of Engineering & Technology, Malakpet, Hyderabad. He is also a member of IEEE.

MOHD ANAS ALI, received B.Tech. Degree in Electronics and Communication Engineering from Pujya Shri Madhavanji College of Engineering & Technology affiliated to JNTU Hyderabad in 2013 & M.Tech. degree in Embedded System from Nawab Shah Alam Khan College of Engineering & Technology. He is presently working at Techno I Security Systems, Abids, Hyderabad.