A Survey on IoT Architectures, Protocols, Security and Smart City based Applications

Parul Datta
Computer Science Engineering Department
Chitkara University
India
parul.datta@chitkarauniversity.edu.in

Bhisham Sharma
Computer Science Engineering Department
Chitkara University
India
bhisham.sharma@chitkarauniversity.edu.in

Abstract-Evolving methodologies are seamlessly connecting the real world and the virtual world using some physical objects and intelligent sensors. Internet of Things (IoT) is one such methodology. Things are becoming smarter than before. IoT empowers users to communicate and control physical devices to salvage vital information. Large amounts of data will be generated and exchanged which in turn will help in decision making. This survey paper describes the architecture of IoT, protocols used in IoT, its security issues and smart city based IoT applications.

***Keywords*—IoT; Data security; Smart city; Protocols**

I. INTRODUCTION

In our everyday life, including our homes and workplace, gadgets have become an imperative part of our life. We are moving towards "anytime anywhere anyone connected to anything" connectivity. With the emergence of advanced technologies like IoT, we are in a "connected" mode to the things around us. Such advancements have crept into our daily lives very sturdily. Through IoT, real world things are a part of the Internet, seamlessly combining physical and digital world. With all this, without a second thought, we can say that IoT is the "Future of Internet". Benefits of IoT are indisputable in every part of life. Development of IoT in current environment foresees many advances in smart cities, smart homes, digital health and other areas as shown in Figure 1 below [1]. IoT boosts connectivity and increases the popularity of mobile communications. IoT is a system that supports large range of applications with contradicting requirements and integrated components. IoT applications include smart infrastructure, smart healthcare, smart governance, smart mobility, smart technology, etc. Amidst all these benefits, IoT services needs to be secured and reliable for day to day applications. Technologies like Bluetooth, ZigBee and Radio Frequency Identification Technology (RFID) enable security in IoT. Overcoming technical challenges requires thorough evaluation of IoT solutions.

With all the advancements in technology, IoT is surely a step ahead of the ancestor technologies in every sphere of life wherever technology is involved.

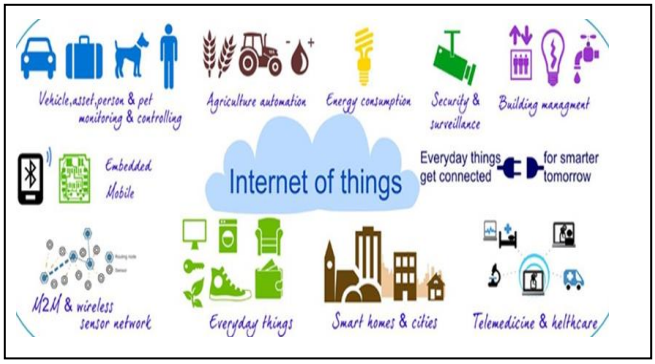

Fig. 1. IoT Generic Application Areas [1]

This survey paper presents an overview of IoT architectures and protocols, its security concerns and its smart city based applications of IoT and is positioned for wide novice audience to give an insight into various aspects of IoT. The rest of the paper is organized as follows. Section II presents review of IoT architecture, protocols and security of IoT. Section III gives smart city based applications of IoT. Section IV compares application layer protocols and security measures of IoT. Finally, Section V concludes the paper.

II. RELATED WORK

A. IoT Architecture

IoT architecture addresses essential factors like Quality of Service (QoS), confidentiality, reliability, integrity, etc. In this section, we will briefly look into the basic and service oriented architecture of IoT. The basic layered architecture of IoT is proposed in [2], [3] and [4] as shown in Figure 2 below [2]. Each architectural layer is briefly described as: The perception layer consists of sensor devices viz, RFID, ZigBee, Quick Response (QR) code, etc. to deal with overall device management and to collect specific information by each type of sensor devices. The network layer forwards information from perception layer to upper layers and keeps sensitive information confidential from sensor devices. Functions of middleware layer are service management and storing lower layer information into the database. The application layer manages IoT applications such as smart health, smart transportation, etc. The business layer covers entire IoT applications and services management.

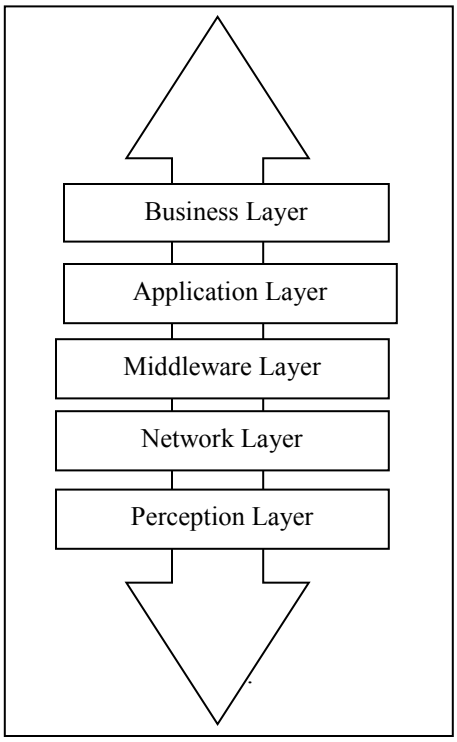

Fig. 2. IoT Basic Layered Architecture [2]

IoT architecture can be service oriented. Its four layers are as shown below in Figure 3 [5]. The sensing layer integrates with hardware. The networking layer supports data transfer over the network. The service layer creates and manages services. The interface layer provides interaction between user and applications.

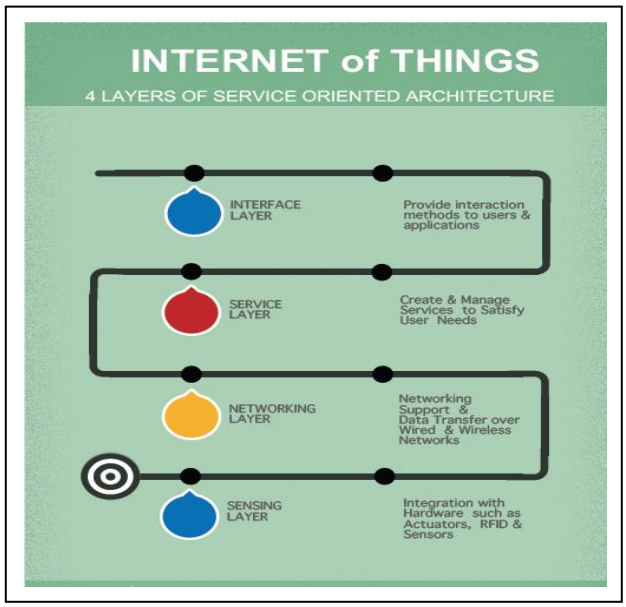

Fig. 3. Service Oriented IoT Architecture [5]

B. *Protocols in IoT*

This section discusses briefly protocols and security measures of IoT.

In a telecommunication connection, end points use a special set of rules and regulations to communicate with other end points in a network. In this section, some of the IoT data protocols are discussed briefly and how they interact with the IoT gateway is shown in Figure 4 below.

Message Queuing Telemetry Transport (MQTT) runs over Transmission Control Protocol/Internet Protocol (TCP/IP) that provides ordered lossless connections. It is a client server messaging protocol which delivers messages with minimized transport overhead [6]. There are three quality of service (QoS) for MQTT protocol viz, 'at most once' which ensures that messages are delivered according to availability of the operating environment, 'at least once' which ensures message arrival and 'exactly once' which ensures message arrival exactly once. MQTT has an astonishing mechanism of notifying an abnormal disconnection.

For constrained nodes and constrained networks, Constrained Application Protocol (CoAP) is used as a web transfer protocol. Constrained nodes often have 8-bit microcontroller with miniature random access memory (RAM) and read only memory (ROM) whereas constrained network results in high packet error rate [7]. Request response interactive model is provided by CoAP and supports built-in services and resources [8]. CoAP meets web requirements like multicasting, minimized overheads and simplicity.

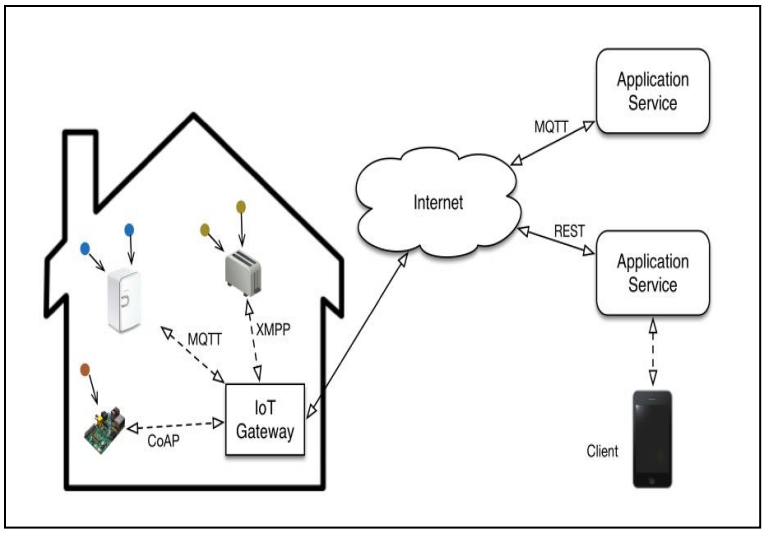

Fig. 4. IoT Protocols [9]

Advanced Message Queuing Protocol (AMQP) is message oriented middleware open standard application layer protocol [10]. Features of AMQP are: message orientation, queuing, routing and security.

Extensible Messaging and Presence Protocol (XMPP) is a protocol for real time communication and is used in applications like voice and video calls etc. [10].

WebSocket provides browser based applications, a two-way communication with server consisting of a handshake followed by message framing [11]. Interaction between browser and web server increases as it facilitates transfer of real time data from and to the server. TCP port number 80 is used for communication. Websocket provides full duplex communication.

C. IoT Security Measures

IoT takes care of security measures by using many technologies as discussed below [12].

- ZigBee: ZigBee is developed by ZigBee Alliance which is standard for personal area networks (PAN) and is two-way wireless communication standard for short range applications [12]. ZigBee provides low cost, low power, reliable communication. ZigBee protocol stack contains four layers as shown below in Figure 5:

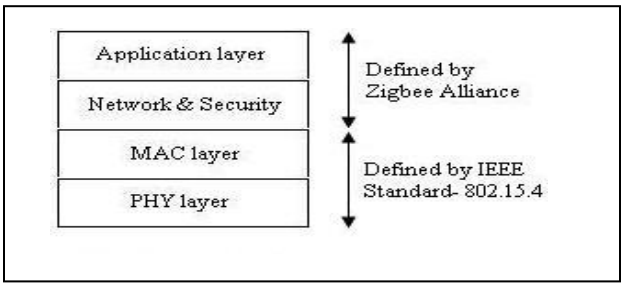

Fig. 5. ZigBee Protocol Stack [13]

ZigBee is positioned on top of Physical and Media Access Control (MAC) layers which are defined by IEEE 802.15.4 standard. ZigBee consists of Application, Network & Security layers. ZigBee interfaces directly with MAC layer which has the following services [12]:

a.) *Access Control*: MAC selects devices to which it needs to communicate depending on MAC address.
b.) *Encryption*: MAC uses symmetric key cryptography to protect data.
c.) *Frame Integrity*: The device which receives data should be able to detect modification in message.
d.) *Messages in Sequence*: MAC prevents replay attacks as MAC frame uses structured series of values.

ZigBee cryptography uses 128 bit keys and Advanced Encryption Standard (AES) encryption [14]. Three types of keys are used:

a.) *Network Key*: It is used in all nodes and is common to all nodes in ZigBee network.
b.) *Link Key*: A secret session key for connected device communication.
c.) *Master Key*: It is used to generate link key.

- Bluetooth

Bluetooth establishes wireless PANs and is an open standard for short range radio frequency communication [15]. There are four security modes in Bluetooth:

a.) *Security Mode 1***:** In this mode, security procedures are never initiated.
b.) *Security Mode 2*: Authorization is introduced in this mode.
c.) *Security Mode 3*: Authentication and encryption is enabled for all connections.
d.) *Security Mode 4*: In this mode, security procedures are initiated after link establishment.

Besides security modes, Bluetooth also provides three encryption modes to provide confidentiality:

a.) *Encryption Mode 1*: Communication is not encrypted.
b.) *Encryption Mode 2*: Individually addressed traffic is encrypted.
c.) *Encryption Mode 3*: All kinds of traffic are encrypted.

Bluetooth technology is prone to networking threats. Some of them are discussed below:

a.) *Bluejacking*: It involves users sending Short Messaging Service (SMS) to other Bluetooth devices. In this, attacker can be saved as contact if content is not appropriately documented. Hence the attacker can send any content which will be automatically opened as it came from a known contact.
b.) *Car Whisperer*: In this attacker, can transmit content to car's speakers or can receive content from microphone in the car.
c.) *Bluesnarfing*: Hackers access Bluetooth devices and get the content of devices through International Mobile Equipment Identity (IMEI) [15].

- RFID

Automatic identification of things and people is done by RFID. RFID has three components viz., tag, reader and back-end database [16]. RFID operates in three frequency ranges Low Frequency (LF), High Frequency (HF) and Ultra High Frequency (UHF). RFID devices are divided into two groups [17]:

a.) *Active*: Active RFID requires power source.
b.) *Passive*: Passive RFID do not require batteries.

RFID encryption levels are Encryption Mode 1: Traffic is not encrypted, Encryption Mode 2: Data Encryption Standard (DES) and Encryption Mode 3: AES-128 bits.
In spite of the above-mentioned encryption modes, RFID have potential security threats as discussed below:

a.) *Clandestine scanning*-In this, RFID tags are scanned without authorization.
b.) *Clandestine tracking*-Chip id is omitted without any information of the holder of the tag.
c.) *Skimming and cloning*-Duplication of tag is possible if tag's secrets are known to hacker.
d.) *Cryptographic weaknesses*-Encrypted data can be decrypted if weak encryption is done.

- WiFi

WiFi allows wireless communication and enables Internet access in the form of radio signals [18]. Possible attacks can be network access control, security of data and network design [19]. WiFi uses six security modes as discussed below [12]:

a.) *Security Mode 1*: Overall security of WiFi network information.
b.) *Security Mode 2*: Wired Equivalent Privacy (WEP), WiFi Protected Access (WPA) and WPA2 encryption.
c.) *Security Mode 3*: MAC addresses filtering.
d.) *Security Mode 4:* Protocol filtering.

e.) *Security Mode 5*: Shield Service Set Identifier (SSID) broadcast information.
f.) *Security Mode 6*: IP address assigning.

WiFi is also vulnerable to many threats viz [12]:

a.) *Wireless Network Eavesdropping:* Information is collected from network by snooping transmitted data.
b.) *Search wireless signal attack*: When a device searches for a wireless network and if the network is not encrypted then it is potentially dangerous to connect to such a network.

III. APPLICATIONS OF IoT

IoT is applicable in every sphere of life. IoT applications are shown diagrammatically in Figure 6.

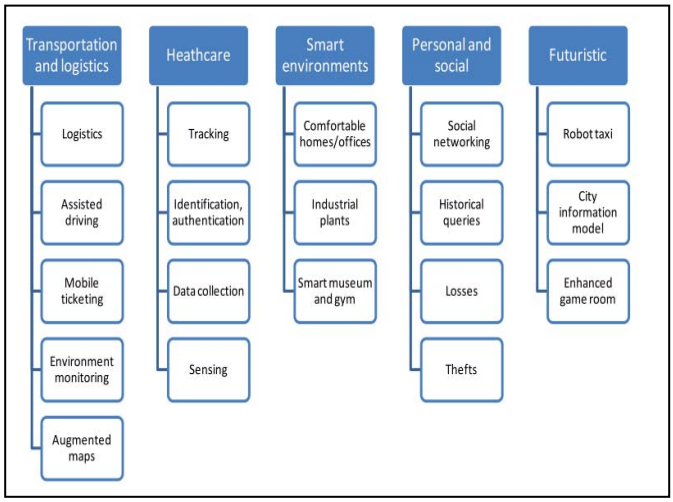

Fig. 6. IoT Applications [23]

Also IoT applications are described briefly below [2]:

- *Assisted Driving*: For better navigation and safety; cars, trains and buses are equipped with sensors and actuators to provide information to drivers and/or passengers about accidents, road closures, etc. [20]. This information can be used to perform route optimization.
- *Mobile Ticketing*: Information regarding transport services can be outfitted with Near Field Communication (NFC) tag [21]. The mobile phone can be hovered over the NFC tag to get information by the user. Information retrieval is done by the mobile phone automatically and suggestion is provided to the user about tickets.
- *Social Networking*: Real-time updating of location about user's activities on social networking websites.
- *Sensing*: Sensors enable devices to diagnose conditions of patients by providing real time information. Continuous monitoring is provided to every patient with multiple wireless technologies.
- *Homes and Offices*: Deployment of sensors in houses and offices makes life easier like room heating can be tailored as per user preferences or weather; alarm and monitoring systems can be implemented, etc.
- *Identification and Authentication*: Preliminary phases of security apply to various phases of healthcare which are used to manage and improve medical staff morale by addressing patient safety issues.
- *Thefts and Losses*: Precious objects can be tagged and their location can be retrieved if the object is moved from a particular constrained area. In this way, probability of loss due to object misplace can be minimized.

IV. COMPARISONS AND DISCUSSIONS

A. This section compares different application layer protocols of IoT in Table I as given below:

Table I. COMPARISON OF APPLICATION LAYER PROTOCOLS

Protocol	Transport	QoS Option	Security	Architecture
MQTT	TCP	YES	TLS/SSL	Publish/Subscribe
CoAP	UDP	YES	DTLS	Request/Response
AMQP	TCP	YES	TLS/SSL	Publish/Subscribe
XMPP	TCP	NO	TLS/SSL	Publish/Subscribe Request/Response

B. This section compares the security measures of IoT included in this paper in Table II as given below [22]:

Table II.COMPARISON OF SECURITY MEASURES OF IoT

Security Measure	Number of Security Modes/Keys	Security Threats
ZigBee	3	Bus Pirate and GoodFet
Bluetooth	4	Bluejacking, Car Whisperer, Bluesnarfing
RFID	3	Clandestine scanning, tracking, Skimming and cloning
WiFi	6	Wireless Network Eavesdropping

V. CONCLUSION

In this paper, we have presented the detailed survey on IoT architectures, protocols, security and smart city based applications. Firstly, we have presented a common IoT architecture that addresses essential factors like QoS, confidentiality, reliability, integrity, etc. by explaining the parts where application layer protocols are required to handle communication. Secondly, we have presented the essential application layer protocols that have attained focus for IoT as well as providing a comparison among each other. Thirdly, we have identified various security measures by using many technologies like ZigBee, Bluetooth, RFID and WiFi. Finally, we have presented various current smart city based IoT applications.

REFERENCES

[1] www.iotworm.com/internet-of-things-applications-area/
[2] S. Kraijak and P. Tuwanut, "A Survey on IoT Architectures, Protocols, Applications, Security, Privacy, Real-World Implementation and Future Trends", 16th International Conference on Communication Technology (ICCT), 2015.
[3] L. Tan and N. Wang, "Future Internet: The Internet of Things", 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010.
[4] M. Wu, T. Lu, F. Ling, J. Sun and H. Du,"Research on the architecture of Internet of Things", 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010.
[5] www.alliedc.com/infographic-what-are-the-4-basic-layers-of-an-iot-service-oriented-architecture/
[6] http://www.mqtt.org/documentation
[7] M. Palattella, N. Accettura, X. Vilajosna, T. Watteyne, L. Grieco, G. Boggia and M. Dohler, "Standardized Protocol Stack for the Internet of (Important) Things", IEEE Communications Surveys & Tutorials, Volume 15, Issue 3, 2013.
[8] C. Bormann, A. Castellani and Z. Shelby, "CoAP: An Application Protocol for Billions of Tiny Internet Nodes", IEEE Internet Computing, Volume 16, Issue 2, 2012.
[9] P. Desai, A. Sheth and P. Anantharam, "Semantic Gateway as a Service Architecture for IoT Interoperability", IEEE International Conference on Mobile Services (MS), 2015.
[10] www.postscapes.com/internet-of-things-protocols/
[11] https://tools.ietf.org/html/rfc6455
[12] M. Grabovica, D. Pezer, S. Popić and V. Knezević, "Provided security measures of enabling technologies in Internet of Things (IoT): A survey", Zooming Innovation in Consumer Electronics International Conference (ZINC), 2016.
[13] www.rfwireless-world.com/Tutorials/Zigbee-protocol-stack.html
[14] K. Masica, "Recommended practices guide for securing Zigbee wireless networks in process control system environments", Lawrence Livermore National Laboratory, 2007.
[15] J. Padgette and K. Scarfone, "Guide to Bluetooth Security Recommendations of the National Institute of Standards and Technology", NIST Special Publication 800-121, 2012.
[16] Md. M. Morshed, A. Atkins and H. Yu, "Privacy and security protection of RFID data in e-passport", 5th International Conference on Software, Knowledge Information, Industrial Management and Applications (SKIMA), 2011.
[17] R. Want, "An Introduction to RFID Technology", IEEE Pervasive Computing, Volume 5, Issue 1, 2006.
[18] Y. Haoyu, "WIFI Technology and Development", Silicon Valley, 2010.
[19] H. Peng, "WIFI network information security analysis research", 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 2012.
[20] L. Atzori, A. Iera and G. Morabito, "The Internet of Things: A survey", Computer Networks Journal, Volume 54, Issue 15, 2010.
[21] K. Bing, L. Fu, Y. Zhuo and L. Yanlei, "Design of an Internet of Things-based smart home system", 2nd International Conference on Intelligent Control and Information Processing (ICICIP), 2011.
[22]www.ciscopress.com/articles/article.asp?p=1823368&seqNum=4
[23] https://blogs.commons.georgetown.edu/cctp-797-fall2013/archives/838