Proceedings of the 23rd International Conference on Automation & Computing, University of Huddersfield, Huddersfield, UK, 7-8 September 2017

A Survey of Internet of Things, Enabling Technologies and Protocols

Muhammad Junaid, Munam Ali Shah, Imran Abbas Satti
COMSATS Institute of Information Technology, Islamabad 44000, Pakistan
Zigron Pakistan (Pvt) Ltd., Islamabad 44000, Pakistan
junaid10293@gmail.com, mshah@comsats.edu.pk, imran.abbas@zigron.com

***Abstract*—One of the popular concepts nowadays is the Internet of Things (IoT). IoT will convert our daily life objects into smart objects. In order to become a part of the IoT network, these smart devices will require some technologies and protocols. In this paper, we will study the different technologies that enable the smart objects to become a part of the IoT network. Furthermore, we will have a look at the architecture of the IoT and discuss the different protocols that have been proposed from time to time.**

Keywords-Internet of Things; Architecture; Standards; Protocols.

I. INTRODUCTION

Internet of Things (IoT) is the interconnection of physical devices with each other in order to facilitate the collection and exchange of data. IoT enables smart objects (devices) to interconnect with each other. The application of IoT allow companies to code and track objects which helps become smarter, efficient speed up their process, reduce errors and prevent theft [1]. The use of IoT can be found in almost all aspects of our life. IoT can be used for energy management, medical and health care, transportation systems, building and home automation and in manufacturing industries. Figure 1 shows an overview of the IoT. IoT facilitates users to bring physical objects into the scope of information technology. This can be achieved by introducing different tagging technologies like RFID, NFC, bar codes and QR codes that allowed user to identify and refer different physical objects.

In Section II, the different enabling technologies that can take part in the IoT are discussed. Section III gives an overview of the architecture of IoT. In section IV, some important IoT protocols are discussed. Section V highlights the importance of standardization in IoT.

II. TECHNOLOGIES FOR IOT

IoT helps in interconnecting different daily life objects. These objects need some elements to become a part of this network. For example, if a book were to be added to the IoT network, we would need a barcode or a NFC tag to uniquely identify the book. Similarly, if a sensor were a part of the IoT network, it would need some wired or wireless medium, such as Bluetooth, to transmit the data it has collected. In this section, we discuss different technologies that could take part or enable an object to take part in IoT.

A. Bluetooth

Bluetooth [2] is a short range radio communication technology which uses radio frequency to provide communication between two devices in an effective range of 10-100 meters. It allows devices such as mobile phones, computers, printers and other smart devices to connect and communicate with a speed of up to 1 Mbps without the need of any physical medium. In IoT, Bluetooth can be used to enable communication between the different objects that are a part of the IoT network. The newer versions of Bluetooth provide high data transfer rates with low power consumption. Due to this reason, Bluetooth technology can be considered as an IoT enabling technology.

B. Barcode and QR-code

Barcode is a machine-readable code that represents some data by lines of varying width and spacing between them. Bar codes are one-dimensional. Later on, using geometric patterns, 2-dimensional codes were introduced. These types of codes are known as QR codes [3]. Barcodes can be used for stock verification in libraries [4], supermarkets, and other similar storage places. Recently, QR-based authentication for ATMs [5] has been proposed which might help in reducing attacks like shoulder surfing.

C. Radio Frequency Identification (RFID)

As the name suggests, RFID [6], [7] is a techniques which uniquely identifies items using radio waves. A RFID system contains a tag, an antenna and a reader. Using the antenna, the reader sends a signal to the tag to get the unique data and the tag replies with its unique data. The tag can be attached to objects such as vehicles, shipment items, books and other items. This enable the items to be uniquely identified and thus part of the IoT network. In this way, the objects can communicate and can be communicated with. RFID can be used in almost every aspect of IoT, like: real-time asset tracking [8] and toll tax payments [9].

D. NFC

Near Field Communication (NFC) [10] is a short range communication technology. It uses magnetic field induction to allow two devices to communicate within a distance of 4cm. Similar to RFID, NFC also operates at a frequency of 13.56MHz. It helps in authentication and authorization. In [11], a method has been proposed for authentication of online banking transaction using NFC enabled mobile devices. Since in IoT we have power-constrained devices, therefore NFC can be of great use.

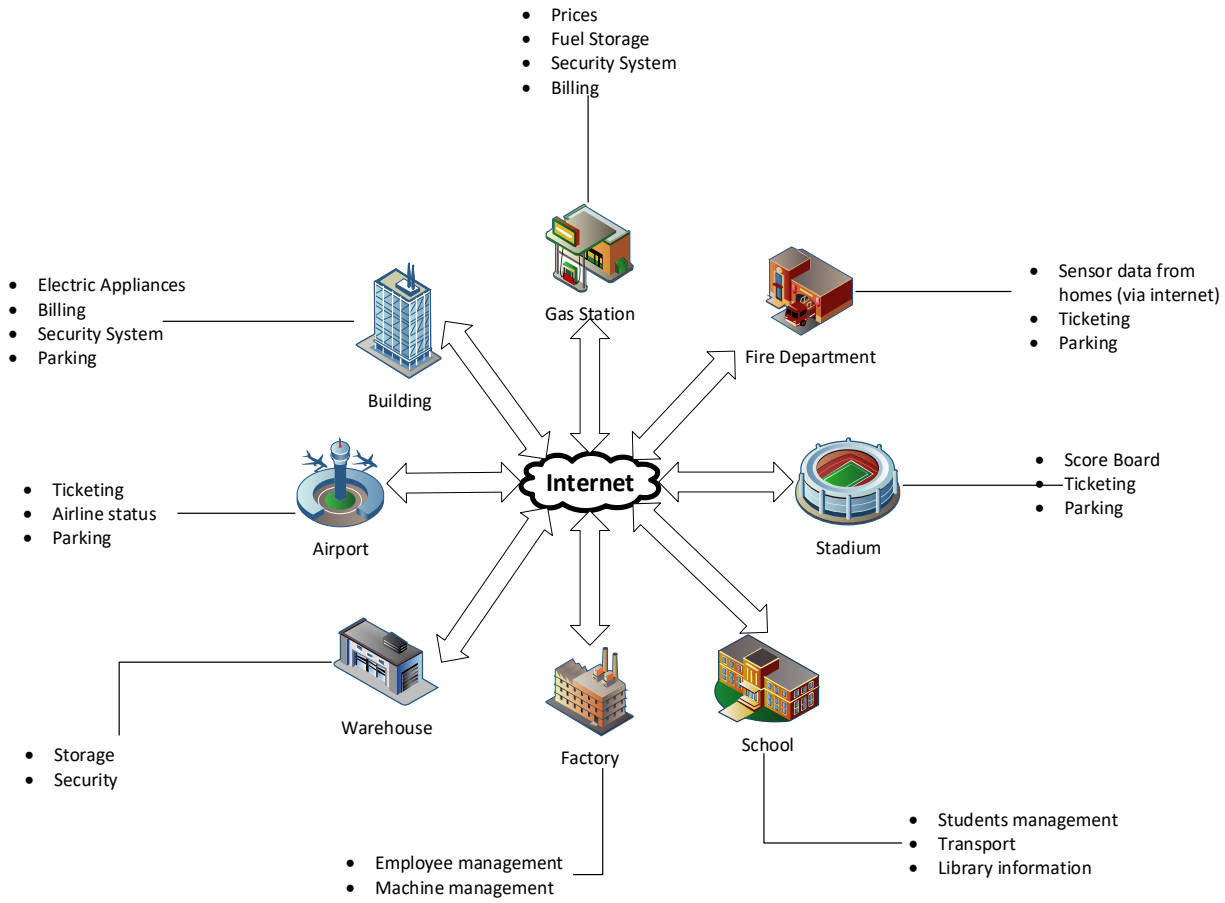

Figure 1: An overview of IoT

III. ARCHITECTURE OF IOT

The importance of IoT can be seen from the fact that IoT will be able to interconnect almost all the daily life objects. Keeping this importance in view, a flexible architecture for the IoT needs to be defined. Many architectures are proposed but a reference model has not been selected yet. A standard architecture for IoT will ensure interoperability, connectivity between heterogeneous devices and security. Meanwhile the Standards Development Working Group of the IEEE Standards Association is working on a project to introduce a standard architecture for the IoT [12].

Here we will discuss the five layered architecture of the IoT [13], [14] that can be seen in Figure 2.

A. Device Layer

This layer consists of the objects that make up the IoT. These objects may be sensors, actuators, mobile devices or any other devices that may help in gathering and processing data. The data collected is passed to the object abstraction layer. The data might be temperature, humidity, binary signal, vibration or any other phenomenon sensed by a sensor. The technologies used at this layer can be sensors, RFID or NFC tags, barcode, QR code or GPS. Some objects cannot transmit data themselves, so these technologies can be implanted using microchips [15].

B. Network Layer

This layer is responsible for transferring data gained from the device layer to the service management layer. The data can be transferred using BLE, RFID, Zig-Bee or any other communication technology.

C. Middleware Layer

The middleware, also known as the service management layer, is responsible for providing services. It identifies the request of a user and provide the required service. This layer is responsible for processing the raw data and generating useful results that can be used for making useful decision.

D. Application Layer

This layer provides the user with the data processed by the middleware. The user request some services and the application layer provides them the service. The application layer cover a large aspect of the market like smart home, smart grids, smart industries, smart vehicle and many more.

E. Business Layer

The business layer is responsible for the management of system activities of the IoT elements. It manages the flow diagrams, graphs and business models based on the data gained from the application layer. It also help users in making decisions based on the analysis of big data.

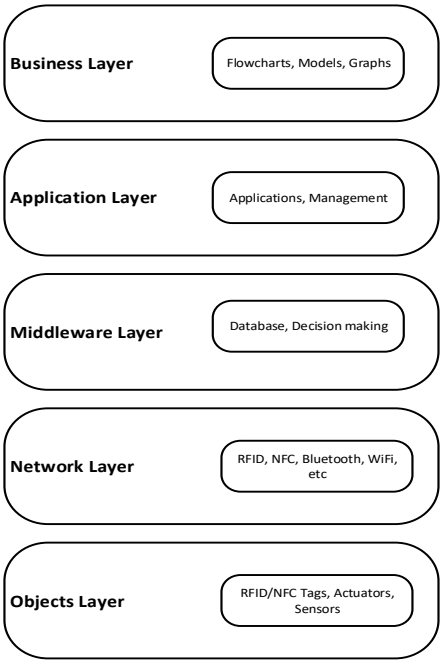

Figure 2: 5-Layered IoT Architecture

IV. PROTOCOLS FOR IOT

A. Constrained Application Protocol (CoAP)

CoAP [16], [17] is an application layer protocol created by the Internet Engineering Task Force (IETF) Constrained RESTful Environment (CoRE). It was designed to provide a lightweight RESTful interface. In terms of power consumption and computation, REST might prove an overhead for lightweight applications such as in IoT. To avoid this overhead, CoAP allows devices to access REST while maintaining their power constraints.

B. Message Queue Telemetry Transport (MQTT)

MQTT is a messaging protocol designed by IBM for remote location connection in bandwidth-constrained environment. The MQTT protocol was standardized by OASIS [18] in 2013. MQTT follows the publish-subscribe architecture. A publish-subscribe architecture consists of a publisher, a subscriber and a broker. The architecture of MQTT can be seen in Figure 3. The publishers are usually sensors that collect data and send it to the broker. The broker is responsible for informing the interested subscribers that new data is available. The publishers go to sleep to as soon as possible after sending the collected data to the broker. Thus, saving battery power.

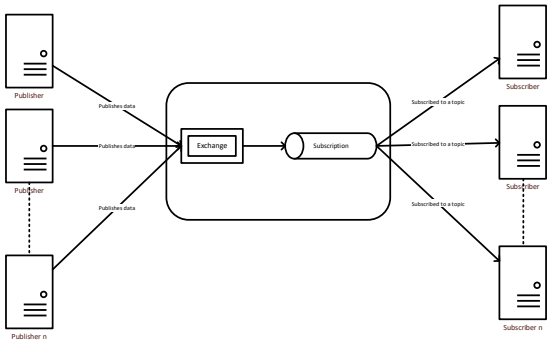

Figure 3: MQTT

C. Secure MQTT (SMQTT)

SMQTT is an enhanced and secure version of MQTT. Since MQTT finds its applications in many aspects of IoT including social, sensor and vehicle networks, therefore it should be secure. In [19], a secure MQTT protocol has been proposed. In this method, the publisher encrypts the data before publishing. The subscriber, after receiving the data decrypts the data. The data is encrypted/decrypted by a key previously provided by the broker. The encryption/decryption mechanism of SMQTT is not standardized. SMQTT is just a proposed protocol to enhance security of MQTT.

D. Advanced Message Queuing Protocol (AMQP)

An enhanced version of MQTT, Advanced Message Queuing Protocol (AMQP) is designed for communication in business and financial industry. AMQP ensures message delivery along with providing TLS/SASL based authentication/encryption. The main difference between MQTT and AMQP is that in AMQP the broker consists of more than one subscriptions (queues). The publishers publish data to the broker that maintains it in a queue (subscription). A subscriber can subscribe to one or more subscription. Figure 4 shows the working of AMQP.

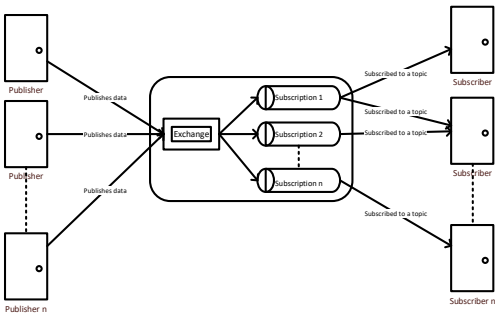

Figure 4: AMQP

E. Extensible Messaging and Presence Protocol (XMPP)

XMPP is a messaging protocol originally designed for real time communication like chatting and in synchronized end-to-end data exchange. XMPP used the Extensible Markup Language (XML) format for communications. XMPP has been standardized by the IETF [20]. XMPP uses a text format of XML for communication, which is an overhead for the network. Due to this reason, it has been rarely used in IoT. However, improving its architecture has gained attention. Recently, a method for compression of XML format using EXI [21] has been introduced. Further improving the compression method may reduce the network overhead, maximizing the use of XMPP.

F. Bluetooth Low Energy (BLE)

BLE, also known as Bluetooth Smart [22], [23] is an energy efficient wireless personal area network technology. It is an upgrade to the traditional Bluetooth. In comparison to its older versions, Bluetooth Smart operates at a very low power transmission power (0.01mW – 10mW) and within a range of 100 meters which is about 10 times that of traditional Bluetooth.

G. Z-Wave

Z-Wave [24] is a low-power wireless communication protocol which supports peer to peer communication up to

30 meters. It is mainly used in Home Automation Networks (HAN). It provides a data transmission rate of 40kbps, however newer versions also support up to 200kbps. Due to its low data transmission rate, it is usually used in remote controlling such as controlling electric appliances, health care control and sensing devices like fire and smoke detection.

H. 6LoWPAN

6LoWPAN [25] is a combination of the latest Internet Protocol with Low Powered Wireless Personal Area Network which is designed to enable low processing devices to transmit data using the internet protocol.

I. IEEE 802.15.4

The IEEE 802.15.4 [26], [27] is an important IoT protocol which specifies a base for the Physical and Medium Access Control (MAC) layer for Low Rate Wireless Private Area Networks (LR-WPAN). It is maintained by the IEEE 802.15 group. The cost and power consumption of IEEE 802.15.4 is low while its message throughput is high. Due to this reason, it is considered as the most feasible for communication in Machine to Machine (M2M), Wireless Sensor Networks (WSNs) and IoT.

J. DASH7 Alliance Protocol (D7AP)

D7AP [28] is a protocol for sensors and actuators which uses the globally available 433, 868 and 915 GHz frequencies. Using these bands, D7AP can operates at a low (9.6kbps), normal (55.6kbps) and high (166.7kbps) rate. Accordingly, its range varies from a hundred meter to a few kilometers. Using the low power wake up mechanism, it minimizes the power consumption and hence enabling its use in power-constrained devices. Recently, D7AP v1.1 has been launched in which the security and interoperability features has been enhanced.

K. LoRaWAN

LoRaWAN is a protocol for Low Power Wide Area Networks (LPWAN). The LoRa Alliance designed it for wireless battery operated devices in Wide Area Networks. It allows secure bi-directional communication and interoperability without any complex setup. LoRaWAN uses Adaptive Data Rate (ADR) techniques to manage the RF output and the data rate to maximize battery life [29].

V. NEED OF STANDARDIZATION

Though the interconnection of devices through Internet have facilitated user in many ways, however, there are some privacy, standardization and legal issues. Researchers are working on various methodologies and protocols to ensure confidentiality, authentication, integrity and the availability of services. At early stages of development, it is hard to decide whether to introduce and define standards or allow user or developers choose which protocol is more suitable for their use. China was the first to ask for standards to be defined for IoT because they claimed that standardization is important [30].

References

[1] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things (IoT): A Literature Review," *J. Comput. Commun.*, vol. 3, no. 5, pp. 164–173, 2015.

[2] H. Fornazier, A. Martin, and S. Messner, "Wireless Communication : Wi-Fi, Bluetooth, IEEE 802.15.4, DASH7," no. march, pp. 1–26, 2012.

[3] T. Marktscheffel, W. Popp, S. D. Fink, and A. Bilzhause, "QR Code Based Mutual Authentication Protocol for Internet of Things," *2016 IEEE 17th Int. Symp. A World Wireless, Mob. Multimed. Netw.*, 2016.

[4] P. V. Danawade, O. Jakate, P. V Yadav, M. Ghori, and V. Kattikar, "IOT Based Stock Verification System Using Raspberry PI , Barcode Scanner and Android Application," vol. 6, no. 6, pp. 6361–6365, 2016.

[5] M. Jacob, R. M. Jose, and N. Mathew, "QR based Card-less ATM Transactions," vol. 2, no. 2, pp. 81–83, 2016.

[6] X. Jia, Q. Feng, T. Fan, and Q. Lei, "RFID technology and its applications in Internet of Things (IoT)," *2012 2nd Int. Conf. Consum. Electron. Commun. Networks*, pp. 1282–1285, 2012.

[7] R. Colella, L. Catarinucci, and L. Tarricone, "Improved RFID tag characterization system: Use case in the IoT arena," *2016 IEEE Int. Conf. RFID Technol. Appl.*, no. 1, pp. 172–176, 2016.

[8] D. Zhang, L. T. Yang, M. Chen, S. Zhao, and S. Member, "Real-Time Locating Systems Using Active RFID for Internet of Things," vol. 10, no. 3, pp. 1–10, 2014.

[9] K. S. Vignesh *et al.*, "RFID Based Automated Tollbooth System," *Imp. J. Interdiscip. Res.*, vol. 2, no. 4, pp. 4–6, 2016.

[10] H. A. Al-ofeishat and M. A. A. A. L. Rababah, "Near Field Communication (NFC)," *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 12, no. 2, pp. 93–99, 2012.

[11] Michelle Fisher, "Conducting an online payment transaction using an NFC enabled mobile communication device.," 2013.

[12] "IEEE SA - IoT Architecture - Internet of Things (IoT) Architecture." [Online]. Available: https://standards.ieee.org/develop/wg/IoT_Architecture.html. [Accessed: 12-Apr-2017].

[13] L. Partra and U. P. Rao, "Internet of things-Architecture, Applications, Security and other Major Challenges," pp. 1201–1206, 2016.

[14] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: The internet of things architecture, possible applications and key challenges," *Proc. - 10th Int. Conf. Front. Inf. Technol. FIT 2012*, pp. 257–260, 2012.

[15] M. Wu, T. J. Lu, F. Y. Ling, J. Sun, and H. Y. Du, "Research on the architecture of Internet of Things," *ICACTE 2010 - 2010 3rd Int. Conf. Adv. Comput. Theory Eng. Proc.*, vol. 5, pp. 484–487, 2010.

[16] Z. Shelby, "The Constrained Application Protocol (CoAP)," 2014. .

[17] M. Castro, A. J. Jara, and A. F. Skarmeta, "Enabling end-to-end CoAP-based communications for the Web of Things," *J. Netw. Comput. Appl.*, vol. 59, pp. 230–236, 2016.

[18] OASIS, "MQTT Version 3.1.1," *OASIS Stand.*, no. October, p. 81, 2014.

[19] M. Singh, M. A. Rajan, V. L. Shivraj, and P. Balamuralidhar, "Secure MQTT for Internet of Things (IoT)," *Proc. - 2015 5th Int. Conf. Commun. Syst. Netw. Technol. CSNT 2015*, pp. 746–751, 2015.

[20] P. Saint-Andre, "Extensible messaging and presence protocol (XMPP): Core," 2011.

[21] P. Waher, "XEP-0322 : Efficient XML Interchange (EXI) Format," 2016.

[22] J. DeCuir, "Introducing Bluetooth Smart: Part 1: A look at both classic and new technologies.," *IEEE Consum. Electron. Mag.*, vol. 3, no. 1, pp. 12–18, 2014.

[23] S. Raza, P. Misra, Z. He, and T. Voigt, "Building the Internet of Things with bluetooth smart," *Ad Hoc Networks*, vol. 57, pp. 19–31, 2016.

[24] "The Internet of Things is powered by Z-Wave." [Online]. Available: http://z-wavealliance.org/. [Accessed: 20-Apr-2017].

[25] V. Gazis *et al.*, "A survey of technologies for the internet of things," *IWCMC 2015 - 11th Int. Wirel. Commun. Mob. Comput. Conf.*, no. September, pp. 1090–1095, 2015.

[26] N. Ahmed, H. Rahman, and M. I. Hussain, "A comparison of 802.11ah and 802.15.4 for IoT," *ICT Express*, vol. 2, pp. 3–7, 2016.

[27] M. Standards Committee of the IEEE Computer Society, "IEEE Std 802.15.4n™-2016, IEEE Standard for Low-Rate Wireless Networks—Amendment 1: Physical Layer Utilizing China Medical Bands," vol. 2016, 2005.

[28] M. Weyn, G. Ergeerts, and R. Berkvens, "DASH7 Alliance Protocol 1.0: Low-Power, Mid-Range Sensor and Actuator Communication."

[29] L. Alliance, "LoRaWAN™ Specification," *LoRa Alliance*, 2015.

[30] R. Van Kranenburg and S. Dodson, "The Internet of Things Dan Caprio Erin Anzelmo Alessandro Bassi," no. October 2015, 2008.