International Journal of Scientific Research & Engineering Trends
Volume 4, Issue 6, Nov-Dec-2018, ISSN (Online): 2395-566X

A Survey on Internet of Things

Research Scholar Deepika. N
Dept. of Electronics and Communication Engg.
Dr. M. G. R Educational and Research Institute
Chennai, India
deepikanarayanamoorthy@gmail.com

Professor Dr. M. Anand
Dept. of Electronics and Communication Engg.
Dr. M. G. R Educational and Research Institute
Chennai, India

***Abstract*-Internet of things is basically a network of devices connected to each other through the internet, which transfers data from one point to another point very quickly. These devices communicate with each other and send data through the network by using communication protocol. At present, IoT devices and their service work using their own architecture and existing protocol stacks and still in the early stage of development. As there are billions of devices connected to the internet, it is hacked easily and personal information is stolen. In this paper we have highlighted various existing application layer protocol MQTT, CoAP, AMQP, XMPP, WEBSOCKET based on their architecture model, power consumption, QOS, security and application. We have also briefly discussed the issues and challenges of internet of things and surveyed the existing techniques.**

***Keywords*-Internet of things, protocols, Architecture, Issues and challenges, etc.**

I.INTRODUCTION

Internet of things (IoT) is a network of physical object which are connected to the internet so that these devices are allowed to send, receive and exchange data. It is a rapidly growing technology with a wide range of applications in many fields like smart homes, smart cities, smart grid, healthcare, agriculture, environmental monitoring, etc. The communication in IoT network can be categorised as people to people, machine to people and machine to machine.

1. People to people (P2P)- Data is transferred between persons and it's called as collaboration connection. Data transfer happens via telephone call, video call or any other social communication.

2. Machine to people (M2P)-data is transferred from machine to users. Information from sensor nodes and computing devices are sent to the user for analysing.

3. Machine to machine (M2M)-data is transferred from one device to another device without human intervention.In the future there will be billions of connections and networks through which anyone can be connected to anywhere through devices likes smart phones , personal digital assistance(PDA) , computers and laptops. This is made possible by using IPV6 which has a larger address space, and provides IP address to each and every object.

According to Gartner there will be more than 25 billion devices connected to the internet by 2020. Though Iot is the recent trend in the next generation technology but it is still in the early stage of development. Implementing an internet of thing system depends upon the layered architecture. Figure 1 show the generic layered architecture of iot [1]. It consists of four layers, of which the top two layers is used for data utilization in application and the lower two layer is used for data capturing

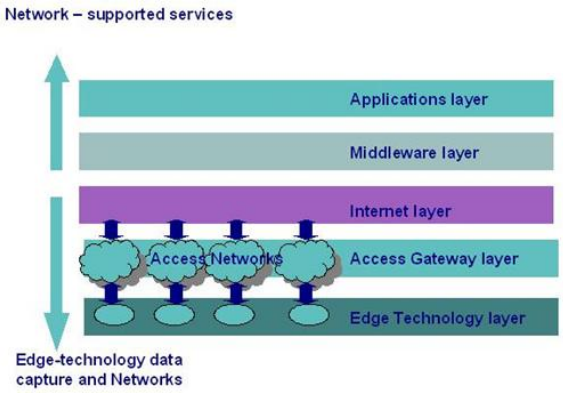

Fig. 1 IoT Architecture

The four layers of IOT Architecture are:

1.Edge layer-It is the hardware layer comprising of sensor network which collects information, embedded system whose processor is responsible for information processing, RFID which provides identification and storage of information .communication, control and actuation are also its other functions

2. Access gateway layer- It takes care of data handling such as message routing, messaging and subscribing.

3. Middleware layer- This layer not only provides interfacing between the hardware and application layer but also responsible for information management, device management, data aggregation, data filtering, access control, EPC and ONS

4. Application layer- This layer is responsible for delivering applications to the user.

II. IOT PROTOCOLS

Internet of things can be defined as domain of constrained devices that sends information and are connected to each other always. These information or data are processed in cloud and analytic results are generated. These results are used to automate action. These devices communicate with each other and send data over the network within a short time and very securely with the help of communication protocol. Selecting communication protocol plays a crucial and vital role. To choose the right communication protocol for our application, certain factors like less power consumption, Security, Small packet size, Operation at low bandwidth, and less transfer time are to be considered. These protocols manage the communication between the gateway, internet and applications. HTTP protocol which helps to browse internet and open web page are used in IoT ,apart from that but there are other efficient IoT protocols that suits low power and constrained devices.

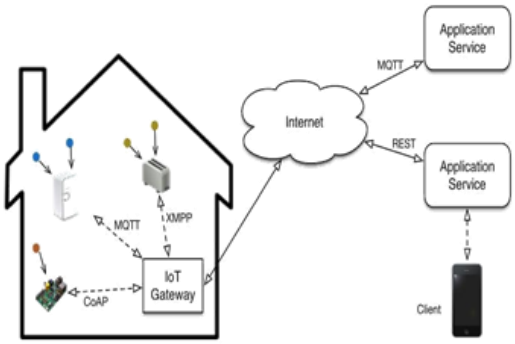

Fig. 2 IoT Protocols

1. Application layer Iot Protocols

1.1Message queuing telemetry transport (MQTT)- MQTT is a simple messaging protocol invented in 1999 by IMB for communication between constrained devices with less bandwidth. It is client server publish/subscribe protocol.

MQTT Publisher: Each client is a publisher which sends information to the broker at a specific topic. Example of MQTT publisher is a sensor or device.

MQTT subscriber: Each client is a subscriber which receives automatic messages whenever there is a new update in a topic he is subscribed .Example of MQTT subscriber is wearable devices.

MQTT Broker**:** MQTT broker is a server that contains topics (4). It receives information, filters information and publishes it to the subscribed client .It demands username/password authentication and ensures security.

MQTT provides three quality of service level, at most once which ensures message is sent once without acknowledgement At least once which ensures arrival of message, with acknowledgement and Exactly once which ensures message is arrived exactly only once . MQTT is light weight, real time, simple, very fast communication with a very less network usage, and highly energy efficient, making this protocol suitable for IoT applications. Face book messenger is built upon MQTT protocol (3). MQTT protocol runs over TCP/IP and it provides lossless, ordered and bidirectional connections. MQTT protocol is required for sending some piece of information constantly.

1.2. Constrained application protocol (CoAP)-it is a web of thing protocol which is specially designed for constrained hardware. It supports web requirements like minimized overhead and multicast. CoAP protocol is required for document transfer. It is inspired by HTPP protocol user can send GET, POST, PUT, DELETE command to server. CoAP runs over UDP that provides fast, ordered and bidirectional connection. It is a request/response protocol where each device acts as client or server.

Two quality of service is Conformable message: It is a request message with acknowledgement, where the response can be sent either synchronously or asynchronously. Non conformable message: it is a message that needs no acknowledgement CoAP is suitable for IOT and M2M communication. As there is no build in security in CoAP, Datagram transport layer security protocol is proposed for authentication, confidentiality, data integrity and cryptographic algorithm (5)

1.3.Advance message queuing protocol (AMQP)- AMQP helps to send and receive messages between applications. It is message oriented middleware open standard application layer protocol (6). Publish/subscribe, point to point and store and forward are the different ways used by AMQP to transfer message .Security in AMQP is handled by TLS/SSL protocols over TCP. It supports various features like security, message orientation routing and queuing.

1.4. Extensible messaging and presence protocol (XMPP)-XMPP is an open standard for user presence and real time messaging. It is request /response and publish/subscribe protocol, which runs over TCP/IP network and has TLS/SSL security. This is a real time communication protocol which is suitable for iot application but does not support M2M communication. XMPP is designed for specific purpose like chatting and messaging. It allows addition of new application on the top of the core protocol. It is used in application like instant messaging, voice and video call, multiparty chat, file transfer (6)

1.5Websocket-web socket allows browser based application. It runs over TCP and it provides security by using web socket over TLS/SSL. It facilitates full duplex communication. The main advantage of websocket is it minimizes communication overhead Websocket uses bidirectional communication. When the client starts handshake with the server (7) the client and server start to exchange message. The session is stopped when the client or the server decide to close the communication Though it is designed for real time application it does not suit constrained devices and thus it does not suit iot application.it provides messaging system by using a sub protocol called websocket application messaging protocol. It is used for real time applications, chatting application and gaming applications.

III. ISSUES AND CHALLENGES

As the number of devices connected to the internet is rapidly increasing, it is facing many challenges in terms of security, privacy, connectivity, compatibility and energy. As we know, the fundamental of internet of things is internet and fundamental technology is wireless sensor network (WSN), therefore the security threats in internet and WSN propagate to the internet of things also. There is different solution to each and every attack. Implementing solutions to these attacks will consume lot of power and creates overheads which in turn will lessen the performance and thus it is difficult task to implement solution to them. Since the interconnected resource is complex, heterogeneous and large in number security in iot is a big challenge. IoT Protocols and standards which are used currently are not capable of handling huge amount of traffic from the smart devices connected to the internet.

The basic requirements of IoT are low power consumption, fault tolerance, optimised algorithm etc. To meet these requirements IoT needs a well-defined architecture that could connect enormous devices to the internet. Though many solutions to these challenges and problems have been proposed by researchers internet of things opens up new horizontal challenges and issues which in turn needs recent research to be addressed. We have summarised the problems and challenges and also existing solutions and techniques of internet of things below.

1. Energy efficiency- the thing in the iot is nothing but the tot devices which is responsible for sensing and monitoring. These devices consists of sensors, hardware and communication platform. Since these sensors operate on batteries, they must be energy efficient. To extend the lifetime of sensors methods like energy harvesting, integrating low power devices and circuit level techniques can be used. Further more suitable lower power communications such as BLE (Bluetooth low power) for short communication range, zigbee for communication between low power device and Ipv6 over 6lowpan to connect constrained devices to internet can be used to meet energy limitations. Tuan Nguyen Gia1 et al (8) has proposed a fog assisted healthcare iot system, the sensor nodes are energy efficient which operates for 155 hours. Implementation of low power CoAP (9) has been proposed to attain high energy efficiency. Lossy signal compression method has been proposed to increase the life time of battery by reducing the size of data of bio signals.

2. Security-IoT networks are constrained in nature and they are often connected to unsecured networks which make the network vulnerable to attacks and easy to be hacked. Iot systems must be designed as a self-healing system which can detect and monitor attacks and also counter measure the attack. Generally security is enforced in application, physical and network layer. Physical attack, network attack, encryption attack and software attacks are performed by attackers to breach security. A. capossele et al (10) has proposed a technique of implementing DTLS over CoAP for iot application to minimise computational overhead.

M. singh et al (11) has proposed secure MQTT which empower security for MQTT and MQTT-SN using CP/KPABE. The proposed PPM algorithm (12) is designed to increase level security and decrease the authentication delay.Confidentiality, authentication, privacy and access control (13) are a few security challenges faced by IoT.

2.1. Confidentiality- ensures that the destination can only read the data. In IoT (14) two way authentications is provided by DTLS (datagram transport layer security protocol)

2.2. Privacy- user information can be easily stolen from device, during communication and processing and also while storing the information. In (15) continuously Anonymizing streaming data via adaptive clustering (CASTLE) scheme is proposed for preserving privacy.

2.3. Authentication-the validity of user is ensured by authentication. To prevent replay and man in the middle attack, an inter device authentication session key distribution system (16) is proposed.

2.4. Access control-user has to give credential details in order to receive access. In (17), the Identity Establishment and Capability-based Access Control (IECAC) protocol with Elliptical Curve Cryptography (ECC) algorithm is suggested for providing the access control. It prevents attacks such as DOS, replay and man in the middle.

3. Fault tolerance- In IoT, tasks are performed by a large number of sensors with are heterogeneous in nature and spread over a wide area. Physical damage, shortage of power or other environmental factors causes failure of sensor nodes. These sensors nodes must recover fast from failure or it may lead to failure of system and affect the performance of the system. In (18) balanced energy adaptive routing protocol (BEAR) has been proposed for IoT networks. In this method location and residual energy information are shared by the sensor nodes, neighbour nodes and successor nodes are elected by the BEAR protocol, and forwarder node is selected based on residual energy. Network life time is improved by 55% by BEAR protocol.

Table1 comparison of challenges in IOT

Challenges	Performance	Advantages
Energy	FOG assisted healthcare system (8)	Energy efficient sensor nodes operates up to 155 hours
	Low power CoAP (9)	High energy efficiency
	Compression of bio signals (19)	Reductions in the signal size of up to 100 times, which involves reductions in the energy
Security	DTLS over CoAP protocol(10)	Minimises computational overhead
	Hybrid parallel partial model (PPM) algorithm (12)	Increase security Decrease authentication delay
Confidentiality	Datagram transport layer security protocol (DTLS) (14)	Increase interoperability
Privacy	Continuously anonymizing streaming data via adaptive clustering scheme (CASTLE) (15)	Prevents privacy risk Efficient
Authentication	An inter-device authentication and session-key distribution (16)	Prevents replay attack and man in the middle attack. Enhanced performance
Access control	An Identity Establishment and Capability-based Access Control (IEAC) protocol with Elliptic Curve Cryptography (ECC) (17)	Prevents man in the middle attack, dos attack and replay attack.
Fault tolerance	Balanced energy adaptive routing protocol (BEAR) (18)	Improved network lifetime by 55%.

VI. CONCLUSION

In this paper we have presented a detailed survey of IoT architecture, issues and challenges and comparison of various IoT protocols. The comparison of IoT protocol shows that the most suitable protocol for IoT application is MQTT and CoAP as they are light weighted and energy efficient protocol which is more suitable for constrained devices. A number of issues and challenges of internet of things have been described and a number of existing techniques like DTLS, CASTLE, BEAR, have been analysed.

REFERENCES

[1]. L. Atzori, A. Lera, and G. Morabito. The Internet of Things: A Survey. Computer Net-works 54(15), 2787-2805. (2010)
[2]. P. Desai, A. Sheth and P. Anantharam, "Semantic Gateway as a Service Architecture for IoT Interoperability", IEEE International Conference on Mobile Services (MS), 2015
[3]. http://mqtt.org/2011/08/mqtt-used-by-facebook-messenger, cited 28 Jul 2014.
[4]. Shinho Lee, Hyeonwoo Kim, Dong-kweon Hong, Hongtaek Ju, Correlation Analy-sis of MQTT Loss and Delay According to QoS Level, International Conference on Information Networking (ICOIN), 28-30 Jan. 2013, pp. 714-717.
[5]. 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.
[6]. www.postscapes.com/internet-of-things-protocols/
[7]. https://tools.ietf.org/html/rfc6455
[8]. Tuan Nguyen Gia1, Mingzhe Jiang1, Victor Kathan Sarker1, Amir M. Rahmani2,3, Tomi Westerlund1, Pasi Liljeberg1, and Hannu Tenhunen,1 " Low-cost Fog-assisted Health-care IoT System with Energy-efficient Sensor Nodes ", 978-1-5090-4372-9/17/©2017 IEEE
[9]. M. Kovatsch, S. Duquennoy, and A. Dunkels, "A Low-Power CoAP for Contiki," in 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems. IEEE, oct 2011, pp. 855–860.
[10]. A. Capossele, V. Cervo, G. D. Cicco, and C. Petrioli, "Security as a CoAP resource: an optimized DTLS implementation for the IoT," Communications (ICC), 2015 IEEE International Conference on, pp. 549–554, 2015.
[11]. M. Singh, R. Ma, S. Vl, and P. Balamuralidhar, "Secure MQTT for Internet of Things (IoT)," Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference on, 2015
[12]. Shailja Dahiya ,Manoj Bohra, "Hybrid parallel partial model for robust & secure authentication in healthcare iot environments ",2017 4th IEEE Uttar Pradesh section InternationalCconference on Electrical,Ccomputer and Electronics (upcon)GLA university, Mathura, oct 26-28, 2017
[13]. A. K. Ashvini Balte, Balaji Patil "Security Issues in Internet of Things (IoT): A Survey," International Journal of Advanced Research in Computer Science and Software Engineering vol. 5, pp. 450-455, 2015.
[14]. T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "DTLS based security and two-way authentication for the Internet of Things," Ad Hoc Networks, vol. 11, pp. 2710-2723, 2013.
[15]. J. Cao, B. Carminati, E. Ferrari, and K. L. Tan, "CASTLE: Continuously Anonymizing Data Streams," IEEE Transactions on Dependable and Secure Computing, vol. 8, pp. 337-352, 2011.
[16]. N. P. a. N. Kang, "Mutual Authentication Scheme in Secure Internet of Things Technology for Comfortable Lifestyle," Sensors, pp. 1-16, 2016
[17]. P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity establishment and capability based access control (IECAC) scheme for Internet of Things," in 15th International Symposium on Wireless Personal Multimedia Communications (WPMC), 2012, pp. 187-191
[18]. N. Javaid, S. Cheema, M. Akbar, N. Alrajeh, M. S. Alabed, and N. Guizani, "Balanced energy consumption based adaptive routing for iot enabling underwater wsns," IEEE Access, vol. 5, pp. 10 040–10 051, 2017
[19]. Mohsen Hooshmand, Davide Zordan, Davide Del Testa, Enrico Grisan, Michele Rossi "Boosting the Battery Life of Wearables for Health Monitoring through the Compression of Biosignals" DOI 10.1109/JIOT.2017.2689164, IEEE Internet of Things Journal.

Author Profile

Deepika.N
Research Scholar, Department of Electronics and Communication Engineering, Dr. M. G. R Educational and Research Institute, Chennai-95.
M.Anand
Professor, Department of Electronics and Communication Engineering, Dr. M. G. R Educational and Research Institute, Chennai-95.