A Review Paper on IOT and it's Data Protocol

Prachi Choubey
B.E Scholar, Dept. of Computer Science and Engg.
Indore Institute of Science and Technology
Indore, India

Margi Patel
Asst. prof. Dept. of Computer Science and Engg.
Indore Institute of Science and Technology
Indore, India

Alpana Meena
Asst. prof. Dept. of Information Technology
Indore Institute of Science and Technology
Indore, India

Abstract— **Lot of google search is filled with the word IOT what does it mean does it really exist or it is virtual. But our future depends on this, it is the base of all artificial intelligence proficiencies. IOT aims to compact everything around us in this world and command and control the system. IOT is just that two or might be more than two devices can talk (interact) to each other. Just things that if your phone tells your house that you are about to reach so just warm up the house or cools it how amazing it can be so just wait for a few years this is about to happen. This is what IOT is all about where the two objects connected to the internet can share the information so that thing becomes easier to human.**

I. INTRODUCTION

Internet of Things describes itself as the wireless network of interconnected objects that can be anything like doors, fans, cooler, washing machine etc. Which can communicate with each other with our intervention. This basically requires few artificial intelligences or when our environment will be embedded with sensor and technologies such as RFID (Radio Frequency Identification), WSN (Wireless Sensor Network), software, actuators etc.

Internet a medium or way to connect the people away distance apart same way the internet of things is interconnection via internet of computing device embedded in day to day objects, enabling all of them to connect together for sending and receiving the data. This includes the object like cell phone, washing machine, air conditioner and doors etc.

The term IOT was first proposed by Kevin Ashton in a presentation to proctor and gamble in the year 1999. At first, he proposed the phrase that internet for things which was later turned to the Internet of Things. It was earlier discussed in 1982 as a concept of network of smart devices as a modification of coke machine where newly loaded cokes were cold [1].

As per the estimate IOT device percent are increasing day by day 31% year-over-year to 8.4 billion in 2017 and it might increase to 30 billion devices by 2020 and its market value is projected to reach up to $7.1 trillion by 2020 or may be more than this [2].

Internet of things could be a vision wherever things (wearable watches, alarm clocks, home device, close objects) become good and practical like living entities by sensing, computing and human action through embedded devices that act with remote objects (servers, clouds, application, services and processes) or person through the web or Near-Field Communication (NFC) etc.

The paper is divided into 5 Sections. Section 2 describes the framework and architecture of IOT. Technologies that enabled IOT to operate in its functional mode is created in section 3. Section 4 represent data access protocols in detail, which is employed in IOT. Section 5 concludes about the paper.

II. EASE OF USE

A. Internet of Things

Internet of Things is that the network of an object or things embedded with natural philosophy, software, sensing element and property to change it to attain nice price and repair by exchanging knowledge with the manufacturer, operator and/or alternative connected device. Every issue is unambiguously diagnosable through its embedded automatic data processing system however is ready to Interoperates at intervals the prevailing net infrastructure [3].

IOT device is sensible and hyper-connected that actually implies that the device may be a state of Unified Communication (UC) during which the traffic handling capability and therefore the information measure of a network perpetually exceeds the demand. The quantity of communication pathways and nodes is far larger than the quantity of subscribers. All devices that might conceivably take pleasure in being connected to the network square measure actually connected. Hyper-connectivity implies that constant property between device, network, server and multiple system.

B. IOT Framework and Platform

The equation below will depict the action and communication of data in successive level in IOT. It manages IOT services using the data from the internetwork of the device and object, internet cloud services and helps to represent the data from the IOT device for managing the IoT cloud server.

Equation:
Gather + Consolidate + Connect + Collect + Assemble + Manage and Analyze = Internet of Things with connectivity to cloud services.

Level 1
Sensors and Smart Sensors

Level 2
Gather Gateway Data Consolidation

Level 3 and 4
Connect + Collect + Assemble + Manage
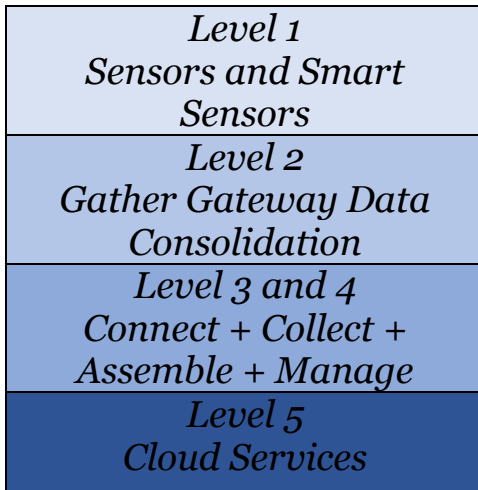
Level 5
Cloud Services

Fig 1: IOT Framework

IBM IOT conceptual framework

This equation represents a complex conceptual framework for IOT using cloud-platform-based processes and services. The specific steps are as follows:

• Level 1 and 2 consist of a sensor network to gather and consolidate the data. First level gathers the data of the things (devices) using sensors circuits. The sensor connects to a gateway. Data is then consolidates at the second stage, for example, transformation at the gateway at level 2.

• The gateway at level 2 communicates the data streams between levels 2 and 3. The scheme uses a communication-management subsystem at level 3.

• An information service consists of connecting, collect, assemble and manage subsystems at level 3 and 4. The services render from level 4.

• Real time series analysis, data analytics and intelligent subsystem are also at level 4 and 5. A cloud infrastructure, a data store or database acquires the data at level 5.

Various conceptual frameworks of IOT find a number of applications including the ones in M2M communication networks, wearable devices, city lighting, security and surveillance and home automation.

C. IOT Architectural view

There is no single consensus on architecture on IOT, which is agreed universally. Different researchers proposed different architectures [4-6].

In that respect are three and five-layer architectures:

The most basic architectures a three-layer architecture. It was inaugurated in the early stages of researchers in this area. It takes in three layers, namely, the perception, network and application layers.
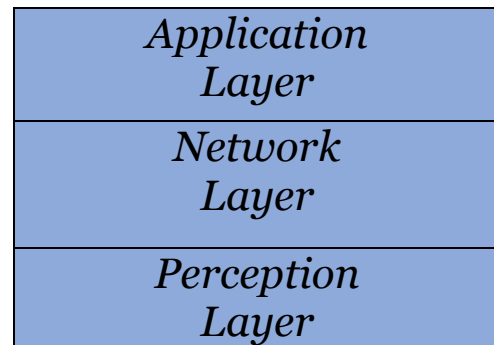

Application Layer

Network Layer

Perception Layer

Fig 2: IOT Architectural View (Three Layer Architecture)

• Perception layer: it is a physical layer, which has a sensor for sensing and gathering information about the environment. It senses some physical parameters or identifies other smart objects in the surroundings.

• Network layer: it is responsible for connecting to other smart things, network devices, and servers. Its features are likewise used for transmitting and processing sensor data.

• Application layer: It is responsible for delivering application specific services to the user. It defines various applications in which the internet of things can be deployed.

Architecture of IOT (A: three layers, B: five layers)

The three-layer architecture defines the principal idea of the IOT, but it is not sufficient for research on IOT because research often focuses on the finer aspects of the IOT. That is why, we give birth many more layered architectures proposed in the literature.

Ace is the five-layer architecture, which additionally includes the processing and business layer. The role of perceptual experience and the application layer is same as the architecture with the three layers. The schema for the other layer is:

• Processing layer: it is also known as the middleware layer. It stores, analyses, and process huge amount of data that comes from the transport layer. It can manage and provide a diverse set of service to the lower stratum. It employs many technologies such as databases, cloud computing, and big data analysis module.

• Transport layer: it transfers the sensor data from the perception layer to the processing layer and processing layer to perception layer through the networks such as wireless, 3G, LAN, RFID, Bluetooth and NFC.

• Business layer: it manages the whole IOT system, including applications, business and profit models, and users' privacy.
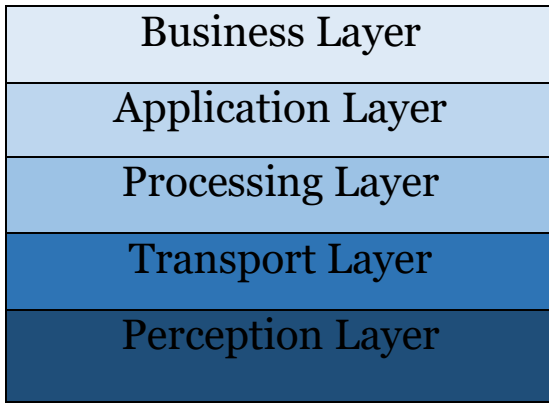
| Business Layer |
| Application Layer |
| Processing Layer |
| Transport Layer |
| Perception Layer |

Fig 3: IOT Architectural View(Five Layer Architecture)

III. TECHNOLOGY BEHIND IOT

Technologies behind IOT:

The IOT is a network of physical objects- vehicles, machines, home, appliances, and more that use sensors and APIs to link up and exchange data over the Internet.

The IOT depends on a whole host of technologies such as application programming interfaces (APIs) that connect devices to the cyberspace.

Another key of IOT technology is big data management tools, Predictive analytics, AI and Machine Learning, Cloud, and Radio Frequency Identification (RFID). Here we will hash out the technologies that can help in the large-scale development of IOT.

A. Radio-Frequency Identification (RFID): It provides a simple low-energy, and versatile option for identity and access tokens, connection bootstrapping, and payments. Radio-frequency identification system uses tags or labels attached to the objects to be keyed out. Two ways radio transmitter- receiver called interrogators or readers send a signal to the tag and read its response. The reader generally transmits their observations to a computer system running RFID software or RFID middleware.

RFID tags are Passive, Active or Battery Assisted Passive. An active tag has an on-board battery and periodically broadcasts its ID signal. A Battery Assisted Passive (BAP) has a small battery on board and is activated when the bearing of an RFID reader. Frequency: 120-150 KHz (LF), 13.56 MHz (HF), UHF, 2450-5800 MHz (microwave), 3.1-10Ghz (microwave). Range: 10cm to 200cm.

Depending on the type of application, RFID frequencies are separated into four different frequency ranges [7], which are given below:

- Low frequency (135 KHz or less).
- High Frequency (13.56MHz).
- Ultra-High Frequency (862MHz 928MHz).
- Microwave Frequency (2.4G , 5.80)

B. EnOcean – ISO/IEC 14543-3-10 (Alliance) [8]: The EnOcean technology is an energy harvesting wireless technology used primarily in building automation system, but as well applied to other applications in industry, transportation, logistics and smart homes. Modules based on EnOcean technology combine micro energy converters with ultra-low power electronics and enables wireless communications between battery fewer wireless sensors, switches, controller and gateways.

Frequency: 315MHz, 868 MHz, 902MHz. Range: 300m Outdoors, 30m Indoors. Examples: wireless switches, sensor and controls.

Nanotechnology: *This technology realizes smaller and* improved version of the things that are interlinked. It can decrease the consumption of a scheme by enabling the development of devices in nanometer scale which can be used as a sensor and an actuator just like a normal device. Such a nano device is made from nano components and the resulting network defines a new networking paradigm which is Internet of Nano-Things (IoNT). There are five nano technologies that are helping the IoNT becomes a reality.

- Nanotubes
- Stretchable electronics
- Bleeding plastic
- Nano-nodes
- Nano-Antennas

C. Networking Technologies: The ability to connect machines, devices, sensors, and other everyday things in an intelligent network and create sense out of them, has huge promises to change everyday life. As can be anticipated by taking in our entire world and attempting to change it one stroke and with one magic wand is unrealistic, challenging and cause for chaos in the short term.

D. Near Field Communication (NFC): NFC is sets of short-range wireless technology typically depend on a distance of 10cm or less. NFC operates at 13.56 MHz in ISO/IEC 18000-3 air interface and at rates ranging from 106 KB/s to 424 KB/s [9]. NFC always involves an initiator and a target, the initiator actively generates an RF field that can power a passive target.

This enables NFC targets to take very simple form factors such as tags, stickers, key fobs, or cards that do not require batteries. NFC hope-to-hop communication is possible, provided both devices are powered. Frequency: 13.56MHz. Range: <0.2m. Examples: smart Wallets/cards, Action Tags, Access control.

E. Bluetooth (SIG): Bluetooth is a wireless technology standard for exchanging data over shorter distances (using short- wavelength radio transmission in the ISM band from 2400-2480MHz) from fixed and nomadic devices, creating personal area networks (PANs) with high level of security. At first, in 1994 Ericson Mobile Communication company started a project called "Bluetooth". It is generally communicating at less than 1 Mbps and Bluetooth uses specification of IEEE 802.15.1 standard. A set of Bluetooth devices sharing a common channel for communication is called Piconet. This Piconet is capable of 2 - 8 devices at a time for data sharing, and that data may be text, image, video and sound. The Bluetooth Special Interest Group comprises more than 1000 companies with Intel, Cisco, HP, Aruba, Intel, Ericson, IBM, Motorola and Toshiba.

Frequency: 2.4GHz. Range: 1-100m. Examples: hand free headsets, key dongles, fitness tracker.

F. Wireless fidelity (WiFi): It is a technology that allows and

electronics device to exchange data wirelessly (using radio waves) over a computer network, including high-speed internet connection. The Wi-Fi Alliance defines Wi-Fi as any wireless local area network (WLAN) product is established at the institute of electrical and electronics engineers (IEEE) 802.11 standards, Wi-Fi Direct, WPS. Vic Hayes has been named as father of Wireless Fidelity. The precursor to Wi-Fi was invented in 1991 by NCR Corporation in Nieuwege in the Netherland. The first wireless products were brought on the market under the name WaveLAN with speeds of 1 Mbps to 2 Mbps.

Frequency: 2.4GHz, 3.6GHz and 4.9/5.0 GHz bands. Range: common range is up to 100mbut can be extended. Applications: routers, tablets.

G. Wireless Sensor Network (WSN): A WSN is a wireless

network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different placements. WSN is a bi-directional wirelessly connected network of sensors in a multi-hop fashion, constructed from several nodes scattered in a sensor field each connected to one or several sensors which can collect the object specific data such as temperature, humidity, speed etc, and then pass on to the processing equipment [10].

IV. DATA PROTOCOLS USED IN IOT

Data protocols in IOT: It is intended for efficiently supporting the big data transfer of host monitoring and control applications, including loading/dumping and remote debugging. It provides packet-based application like remote loading and debugging with an efficient, trusted data transport service. The primary objective of RDP is to remain effective in environments where there could be a non-

sequential message-segment delivery or prolonged transmission delays and loss.

Key goals of data protocols are:

- To represent a full-duplex communications channel between the two hops of every transport connection.

- To precisely transport every user message and to report a message delivery, abortion to the user in case the message transfer abort.

- To discover and abolish any defective or duplicate segments. In order to fulfil this task, RDP employs a checksum and sequence number in every segment header.

- To optionally offer sequenced segment delivery. Sequenced segment delivery should be described at the time a connection is gained.

- To acknowledge the segments acquired from a sequence, as they get in. This consequences in the freeing up of resources on the sending side.

There are various different data protocols to opt for when it comes to connecting various devices to the internet of things. Few are new while few are older and legacy protocols. Depending on various implementations and sensors, use of protocols differs. Each one experiences, their own strength and weakness. It is important to stick to open standards for maximum interoperability between devices and applications.

A. MQTT (Message Queuing Telemetry Transport): It is An

ISO standard (ISO/IEC PRE 20922) Publisher-subscriber (It is a messaging pattern where senders of messages, called the publisher, do not program the message to be posted directly to specific receivers called subscriber, but instead categorize published messages into classes without knowledge of which subscribers, if any, there may be) based messaging protocol. Andy Stanford Clark of IBM and Arlen Nipper of Cirrus Link Authored the first edition of the protocol in 1999. In 2013, IBM presented MQTT V3.1 to the OASIS specification body with a charter the ensured only minor alterations to the specification could be accepted [12].

It operates on top of the TCP/IP protocol. It is designed for connections with remote locations where a "small code footprint" is required or the network bandwidth is restricted. It is a protocol that was specifically created for SCADA system (what is SCADA System it is Supervisory Control and Data Acquisition is a control system architecture that uses computers, networked data communication and graphical user interfaces for high level process supervisory management). It uses a publish/subscribe mechanism to minimize the load and overhead with application-specific, custom JSON or binary formats.

MQTT is widely undertaken in IT departments worldwide, with many open source examples available in just about any programming language. It has many key definitions: client, broker, topic

- MQTT client is any device from a micro controller up to a full-fledged server, that has an MQTT library running and is plugged in to an MQTT broker over any kind of network.

- The broker is primarily responsible for receiving all messages, filtering them, decide who is interested in it and then beaming the message to all subscribed clients.

- Messages are published to an address called topic. Clients subscribe to topics and "listen" to them receiving every message that's published to a topic. Topics in MQTT have a hierarchical structure. But there is an opportunity to use Wildcards "+" and "#". "+" refers to a single directory, while "#" matches any number of them.

- MQTT has several useful features like Last Will and Testament Message and Retained Messages. When a client disconnects unexpectedly, a broker sends a message to all subscribed to a topic client. Retained message updates of newly connected clients with a status update.

MQTT brokers may require username and password authentication from clients to connect. To ensure privacy, the TCP connection may be encrypted with SSL/TLS. There are also 3-levels of QoS.

B. CoAP (Constrained Application Protocol): It is an

application layer protocol that is intended for use in resources-constrained internet devices such as WSN nodes. CoAP is designed to easily translate to HTTP for simplified integration with web, while also meeting specialized integrations such as multicast support, very low overhead and simplicity. The Internet Engineering Task Force (IETF) Constrained RESTful environment Working Group (CoRE) has served the major standardization work for this protocol. In lodge to make the protocol suitable to IoT and M2M application, various new functionalities have been added [12].

The CoRE group has proposed the following feature for CoAP: RESTful protocol design minimizing the complexity of mapping with HTTP, Low header overhead and parsing complexity, URI and content-type support, Support for the discovery of resources provided by known CoAP services. Simple subscription to a resource, and resulting push notifications, Simple caching based on max-age." It is a document-oriented protocol which is designed for constrained devices.
CoAP uses a client/server model where clients send requests to servers and servers respond to Clients. Clients may use GET, PUT, POST and DELETE resources. Messages in CoAP can be "confirmable" or "non-confirmable".

In CoAP is available content negotiation. To show a preferred representation of a resource clients use Accept option, and servers respond with a Content-Type. This allows the client and the server evolve independently from each other.

CoAP Protocol provides its users with the ability to observe a resource. It means that after removing the initial document, a server may keep on replying. You just require to set the observe flag on a CoAP GET request. It allows clients to receive state changes if they happen.

Because CoAP is built on top of UDP not TCP, SSL/TLS are not available to provide security. DTLS, Datagram Transport Layer Security provides the same assurances as TLS, but for transfers of data over UDP.

C. AMQP (Advance Message Queuing Protocol): It is an

open standard application layer protocol for message-oriented middleware. The determining feature of AMQP is message-oriented, queuing, routing (including point-to-point and publish-subscribe), reliability and security. AMQP rise in 2003 by John O'Hara at JPMorgan Chase in London. AMQP were conceived as a cooperative open effort. The initial conception was by JPMorgan Chase from mid-2004 to mid-2006 and its contracted iMatix Corporation to develop a C broker and protocol documentation. AMQP mandates the behavior of the messaging provider and the client to the extent that implementations from different vendors are interoperable, in the same way as SMTP, HTTP, FTP etc. Have created interoperable systems. AMQP is a wire-level protocol (a wire level protocol is a description of the format of the data that is shipped across the network as a stream of bytes).

AMQP is a binary application layer protocol that was generated to substantiate a huge number of messaging applications and communication designs. It comes-up with flow-controlled, message-oriented communication with built-in options for message delivery guarantees, In addition, authentication and/or encryption based on widely accepted Internet authentication and data security protocols a like Simple Authentication and Security Layer (SASL) and/or Transport Layer Security (TLS).

AMQP is the prime transport layer protocol used by the Azure IoT Hub. AMQP defines a self-describing encoding scheme allowing interoperable representation of a wide scope of commonly used types. It also permits typed data to be annotated with additional meaning.

D. WebSocket: It is a computer communication protocol,

unlike http provide full-duplex (bi-directional) communication channel over a single TCP connection. The WebSocket protocol was standardized by the IETF as RFC 6455 in 2011, and the WebSocket API in Web IDL is being standardized by the W3C. It enables streaming of message on top of TCP. WebSocket was invented by Ian Hickson and Michael Carter. WebSocket was first referenced as TCP Connection in the HTML5 cataloguing, as a procurator for a TCP-based socket APIs. In June 2008, a series of conversation were led by Michael Carter that resulted in the first version of the protocol known as WebSocket.

WebSocket is currently one of the main players in the Realtime (low-latency) world. WebSockets gurantee, persistent connections with simultaneous bi-directional communication. They come with all the benefits of HTTP since WebSockets initially start off as an HTTP handshake, before getting kicked upstairs to continue the rest of the communication in WebSockets. The very quintessence of WebSockets is a push-based strategy. It supports publisher/subscriber paradigm because it keeps the connection open until deliberately closed by one of the two parties under communication (i.e. Client or a Server).

Application of WebSocket: A WebSocket is a low-latency (real-time), full-duplex (bidirectional), long-running (persistent), single connection (TCP) between a client and server. WebSockets provide a huge benefit for real-time, event-driven web applications and are becoming more common to power real-time data updates and synchronization, live text chat, television conferencing, VOIP, IoT control and monitoring. They are habituated for a variety of apps in gaming, social and collaborative networks, logistics, finance and home, vehicle and industrial automation to name a few. Most major web browsers currently support their exercise.

V. CONCLUSION

In this survey paper we presented a framework, architecture, technologies enabling IOT and current protocols on IOT mainly focused on Data Protocols. The technologies in the core infrastructure layer are showing signs of maturity. However, there are a lot more things to be searched in the area of IOT applications and communication technologies. With the incessant burgeoning of the emerging IOT the concept of Internet of Things will soon be inexorably developing on a very large scale. These fields will surely make an impact on human life and their future aspects.

REFERENCES

1. **"Internet of Things"** Wikipedia official blog it can be accessed at: https://en.wikipedia.org/wiki/Internet_of_things.
2. **"trends and characteristic of Internet of Things"** Wikipedia official blog it can be accessed at: https://en.wikipedia.org/wiki/Internet_of_things.
3. **Jen Clark** in November 17, 2016 **"What is Internet of Things"** this blog can be accessed at: https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/.
4. I. Mashal, O. Alsaryrah, T.-Y. Chung, C.-Z. Yang, W.-H. Kuo, and D.P. Agrawal, "**Choices for interaction with things on Internet and underlying issues**," Ad Hoc Networks, vol. 28, pp. 68–90,2015.
5. O. Said and M. Masud, **"Towards Internet of Things: survey and future vision,"** International Journal of Computer Networks, vol. 5, no.1, pp.1–17, 2013.
6. M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, **"Research on the architecture of internet of things,"** in Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE '10), vol. 5, pp. V5-484–V5-487, IEEE, Chengdu, China, August2010**.**
7. L.G. Guo, Y.R. Huang, J. Cai, L.G. QU, "**Investigation of Architecture, Key Technology and Application Strategy for the Internet of Things,"** in Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC), 2011, Volume: 2, pp. 1196-1199.
8. Postscapes **"IoT Technology Guidebook"** an overview to what makes up Internet of Things (IoT) systems and devices. This can visit at: https://www.postscapes.com/internet-of-things-technologies/.
9. Somayya Madakam, R. Ramaswamy, Siddharth Tripathi. **Internet of Things (IoT): A Literature Review**, January, 2015.