INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue2)
Available online at www.ijariit.com

Enabling Technologies, Protocols, and Applications: A Detailed Survey on IOT

Gururaj Kulkarni
KLS GIT Belagavi
gururaj@git.edu

S. H Manoor
KLS GIT Belagavi
shmanoor@git.edu

P. V Mitragotri
KLS GIT Belagavi
pvmitragotri@git.edu

Abstract: ***The Internet of things is used as a parasol catch word for combining and covering the major aspects related to the extension of the Internet and Web into the phenomenon, by means of vast positioning of spatially distributed devices that contains embedded identification, sensing and/or actuation capabilities. Internet of Things (IoT) consists of a large number of connected objects that are communicating with each other. To discuss the Internet of things in wider sense and precedence on protocols, technologies, and application along with related issues. The main factor IoT concept is the integration of different technologies. The IoT is empowered by the hottest developments in RFID, smart sensors, communication technologies, and Internet protocols. The primary hypothesis is to have smart sensor dealing directly to deliver a class of applications without any external or human participation. Recently development in the Internet and smartphone and machine-to-machine technologies can be considered the first phase of the IoT. In the platinum should continue to raise IoT is expected to be one of the main hubs between various technologies by connecting smart physical objects together and allow different applications in support of smart decision making. In this paper, we discuss IoT architecture and the technical aspect that relate to IoT. Then, give an overview of IoT technologies, protocols and applications and related issues with a comparison of other survey papers. The survey aims to help other researchers in delving into the details of such techniques by going through their classification and comparison. The classification has been done based on the inherent features of this authentication technique such as being distributed vs. centralized, flat vs. hierarchical, and more others.***

Keywords: Internet of Things (IOT); IOT, Gateway; Authentication Techniques; Security Attacks; IOT Architecture; Www.

I. INTRODUCTION

Nowadays, around two billion people around the world use the Internet for browsing the Web, sending and receiving emails, accessing multimedia content and services, playing games, using social networking applications and many other tasks. While more and more people will gain access to such a global information and communication infrastructure, another big leap forward is coming, related to the use of the Internet as a global platform for letting machines and smart objects communicate, dialogue, computer and coordinate. It is predictable that, within the next decade, the Internet will exist as a seamless fabric of classic networks and networked objects. Content and services will be all around us, always available, paving the way for new applications, enabling new ways of working; new ways of interacting; new ways of entertainment; new ways of living. In such a perspective, the conventional concept of the Internet as an infrastructure network reaching out to end-users terminals will fade, leaving space to a notion of interconnected ‘‘smart’’ objects forming pervasive computing environments. The term Internet of Things (IOT) has been known for last few years. In recent time, it’s getting more attention due to the advancement of wireless technology. The basic idea is due to a variety of object- such as RFID, NFC, Sensors, actuators, mobile phones, etc. which can interact with each other by having a distinct address. The IoT empowers substantial objects to see, hear, think and per- form jobs by having them “talk” with each, to share information and to synchronize pronouncements. The IoT transforms these objects from being conventional to smart by manipulating its underlying technologies such as omnipresent and pervasive computing, embedded devices, communication technologies, sensor networks, protocols, and applications. When IoT was introduced, Radio frequency (RFID) seemed to be necessary for it. There are various technologies similar to RFID, Near Field communications (NFC), Machine to Machine (M2M) and vehicular to vehicular communications (V2V), which can be used to implement the modern idea of IoT [1]. The life of potential user can become easy and comfortable by adopting various technologies based on IoT. In addition, IoT has a dramatic effect on domestic spheres, such as assisted living, smart homes, smart cars, etc.

In the business sector, IoT has noticeable advancement in manufacturing and service industry such as better services, more production, and superior quality. The worldwide adoption of above-mentioned technologies does appear smooth but involves lots of issues, that needed to be solved before it worldwide acceptance. The major issues that IoT is of security because of Internet hackers. Some other problems of IoT are standardization issues, addressing problems and scalability problems etc. Therefore, research is needed to resolve these complicated issues. This paper will enable the reader to have a basic understanding of IoT, its technologies, and applications and the open issues that IoT is facing which needed to resolve for near future.

We do believe that this fragmentation is potentially harmful to the development and successful adoption of IoT technologies. We, therefore, hope this survey can help in bridging existing communities, fostering cross-collaborations and ensuring that IoT-related challenges are tackled within a system-level perspective, ensuring that the research activities can then be turned into successful innovation and industry exploitation.

II REFERENCE MODEL OF IoT ARCHITECTURE

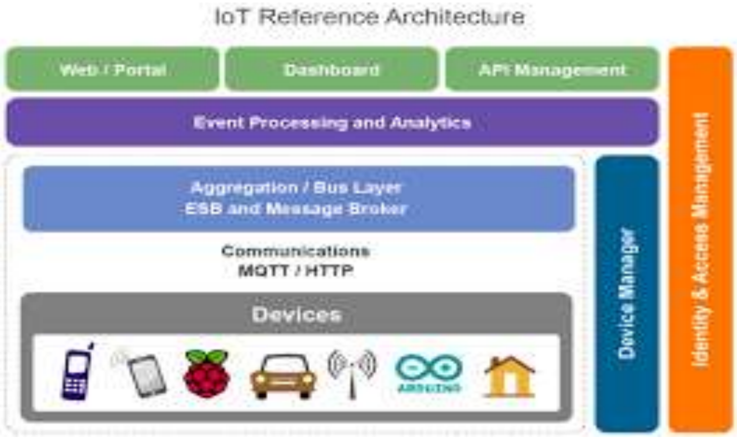


Fig 1: Reference Architecture of IOT

VISION BEHIND THE REFERENCE MODEL OF IOT

In the vision of the Internet of Things, IoT-A wants to promote, a high level of interoperability needs to be reached at the communication level as well as at the service and the information level, going across different platforms, but established on a common grounding. The IoT-A project reckons that achieving those goals comes in two steps, first of all in establishing a common understanding of the IoT domain (hereafter called Reference Model), and second in providing to IoT system developers a common foundation for building interoperable IoT system Architectures (hereafter called Reference Architecture). A Reference Architecture (RA) can be visualized as the “Matrix” that eventually gives birth ideally to all concrete architectures. For establishing such a Matrix, based on a strong and exhaustive analysis of the State of the Art, we need to envisage the superset of all possible functionalities, mechanisms and protocols that can be used for building such concrete architecture and to show how interconnections could take place between selected ones (as no concrete system is likely to use all of the functional possibilities). Giving such a foundation along with a set of design choices, based on the characterization of the targeted system w.r.t. various dimensions (like distribution, security, real-time, semantics,...) it becomes possible for a system architect to select the protocols, functional components, architectural options, ... needed to build their IoT systems.

The ultimate aim of the Reference Architecture work is to make sure that concrete system designers will eventually use it. High attention is therefore paid to ensuring the soundness of our work. In particular, this version of the ARM aims at making more explicit the various links existing between the various models, views, and perspectives so that it will Make the work of systems designers easier.

The vision summarizes the rationale for providing an architectural reference model for the IoT. At the same time, it discusses underlying assumptions, such as motivations. It also discusses how the architectural reference model can be used, the methodology applied to the architecture modelling, and the business scenarios and stake-holders addressed. Business scenarios defined as requirements by stakeholders are the drivers of the architecture work. With the knowledge of businesses aspirations, a holistic view of IoT architectures can be derived. Furthermore, a concrete instance of the reference architecture can be validated against selected business scenarios. A stakeholder analysis contributes to understanding which aspects of the architectural reference model need to be described for the different stakeholders and their concerns. According to common usage, this part constitutes a subset of the vision.

Several trends have emerged over the past several years that are working together to shape the emerging IoT market:

- Rapid growth of data and analytics capabilities enabled by cloud computing
- Rapid growth in smart mobile devices
- Increasing interconnectivity between industrial, operational, and smart mobile devices
- Convergence of industrial and enterprise networks that enable applications such as video surveillance, smart meters, asset tracking, fleet management, digital health monitoring, and a host of other next-generation connected services.

III INTRICATE TECHNOLOGIES

Various technologies are involved implementing the idea of IOT. In this paper, we will focus on these. Radio frequency identification (RFID) Near Field Communication (NFC). Machine-to-Machine Communication (M2M)

- Vehicle-to-Vehicle Communication (V2V)

A. Radio frequency identification (RFID) RFID system comprise of one or more readers and several RFID tags. It uses radio frequency electromagnetic fields to send data attached to it. The tags that are attached to it, stored data electronically which can be read by RFID when it comes in the proximity of the reader comments. RFID allows monitoring objects in real time, without the need of being in the line of sight comment RFID tag or label is very small microchip attached to an antenna in a compact package. These tags antennae receive a signal from RFID and return it with some extra information [11]. Hitachi has developed a tag with dimension. The RFID tag comes in three configurations, Passive Reader Active Tag (PRAT), Active Reader Passive Tags (ARPT) and Active Reader Active Tag (ARAT). In ARAT, the reader is passive and receives the signal from the battery operated tag and its transmission range is from 1-2000 feet depends upon architecture. Secondly, most commonly used configuration, ARPT does not have onboard supplies, so it consumes the energy required to send data from the query signal sent by the RFID reader [11]. The last one, ARAT have both the reader and tags active, and tags only awoke by the reader when it comes under the domain of reader. Transmission may appear in different frequency bands spanning low frequency (LF) at 124-135 KHz up to ultra- high frequency (UHF) at 860-960 MHz an Electronic Product Code (EPC) is one common set of data stored in a tag. The objects can be tracked uniquely because EPC's are coded on RFID tags. It contains a 96-bit string of data. The first bits of this string are known to identify the version of the Protocol [12]. The next 28 bits are fixed to identify the organizations that are handling this tag and this organization id is assigned by EPC global consortium. The next 24 bits are an object class, identifies the kind of product. Further last 36 bits are a unique serial number of a particular tag. As compare to URL, the entire electronic product code number can be used as a key into a global database to uniquely identify a particular code.

B. near Field Communication It is similar to RFID configuration. NFC can be made customer-oriented by integration of RFID reader into mobile phones. In addition, it is the type of radio communication between NFC mobile devices by connecting them together in the domain of another phone. It is short range, low power Smart Grid Application Bandwidth Latency Substation Automation 9.6-56 kbps 15-200 ms WASA 600 – 1500 kbps 15-200 ms Outage Management 56 kbps 2000 ms Distribution Automation 9.6-100 kbps 100 ms-2 sec Distributed Energy Resources 9.6-100 kbps 100 ms-2 sec Smart Meter Reading 10-100 kbps/meter 500 kbps/concentrator 2000 ms Demand Response 14 – 100 kbps 500 ms/min Demand Side Management 14 – 100 kbps 500 ms/min Assets Management 56 kbps 2000 ms 382 wireless link that can send small amounts of data between two devices within the range of lying in the specific domain [13]. No paring is needed before the actual sending of data in comparison to Bluetooth [14] [25]. NFC operates within the unlicensed Radio Frequency band of 13.56MHz. The typical range of NFC is 20m and mostly it depends on the size of the antenna in the device. The NFC technology can play a significant role in the future progress of IoT. It will enable to provide necessary tool to be wirelessly connected to other smart objects [15]. For example, by using NFC mobile a user will be able to transfer the mobile set into other various objects like the mobile set will be able to used as a credit card.

C. Machine to Machine (M2M).

It refers to the communications between computers, embedded processors, smart sensors, actuators and mobile devices. This sort of communication is increasing these days. There are four components of M2M, that are sensing, heterogeneous access, information processing and applications & processing. In actual, M2M is a five-part structure that is as followsM2M Device: A device capable of replying to request for data contained within that device [16]. 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 [17].M2M Applications: Contains the middleware layer where data goes through various application services and is used by the specific business processing engines. M2M Applications: Contains the middleware layer where data goes through various application services and is used by the specific business processing engines. It has applications in different sectors like healthcare, smart robots, cyber transportation systems (CTS), manufacturing systems, smart home technologies, and smart grids [18].An example of M2M area network typically includes personal area network technologies, such as Ultra-wideband and Bluetooth or local networks.

D. Vehicle-to-Vehicle Communications (V2V).

V2V communications involve a vehicle, which acts as a node in a network and communication is done by the use of various sensors connected to an ad-hoc network. The infrastructure of this network is quite complicated because there is no any fixed topology to be followed as the vehicle is moving from one place to another all time. There are four wider categories of this network, namely safety and collision avoidance, traffic infrastructure management, vehicle telemetric, and entertainment services and Internet connectivity [19]. Vehicles communicate with each other within the range of 1000m. Two types of communications are there: the first one is called vehicle to vehicle and other is related to road infrastructure. Intelligent transport system

(ITS) is related to the vehicular communication system. According to an architectural aspect, it focuses mainly on routing protocols that are a Physical layer (PHY), Medium Access Control MAC layer, and broadcasting [19].

IV. APPLICATIONS

Applications of IoT are very diversified. Applications of IoT are increasing every day in many domains. Every day individual /industrial changes our needs and as per need, we use the Internet and hence Internet-of-Things. There are plenty of applications of IOT. In coming years, IOT will be more revolutionized because of the RFID, NFC, M2M and V2V communications.

A. Radio frequency Identification (RFID)

1) Smart parking

In recent time, smart parking sensors are attached in parking space to detect the arrival and departure of vehicles. It provides an efficient management solution which helps motorist to save time and fuel. It provides motorists with accurate information about parking spaces and keeps the traffic system smooth. It also enables the facility of deployment to book parking space directly from the vehicle. It can also help to reduce CO2 emission and lessen the traffic jams [20].

2) Augments maps

Tourists augmented maps with tags allow NFC tag would enable the phones to search the information about places by connecting to web service. By this one will be able to search required information about hotels, restaurants, monuments, theater and the local attractions. This can be 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 [21].

3) Logistics

By implementing IoT in retail chain monitoring has many advantages: RFIC and NFIC can be used to monitor every detail such as commodity details, purchasing of raw materials, production and sales of the product after sale service. With the help of IoT, one can track the inventory in the warehouse so that one can have information about stock, customer's satisfaction etc. and result in increased sales [21].

4) Data collection

If doctor becomes enable of having collection and transfer of data then it would help in reducing them, minimizing the data collection error, automated care, and routine auditing. It will also enable to transfer the previous health record of patients, which would result in an accuracy of the medication given by doctor [20].

5) Smart water supply

Wireless network system will enable to monitor the water supply and will help to ensure that there is the adequate water supply for the resident and business use. It will also help to discover if there is any water loss. In this way, water leakage problem would be discovered and help in water saving. Tokyo, for example, has calculated they save $170 million each year by detecting water leakage problems early [22]. 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.383

6) Smart homes and offices

In recent time, human life is surrounded by thousands of electronic gadgets like microwave ovens, refrigerators, heaters, air conditioners, fan, and lights.

V. STANDARD PROTOCOLS BEHIND IOT

The Internet revolutionized how people communicate and work together. It ushered in a new era of free information for everyone, transforming life in ways that were hard to imagine in its early stages. But the next wave of the Internet is not about people. It's about intelligent, connected devices.

To interact successfully with the real world, these devices must work together with speeds, scales, and capabilities far beyond what people need or use. The Internet of Things (IoT) will change the world, perhaps more profoundly than today's human-centric Internet.

Protocol Overview

Devices must communicate with each other (D2D). Device data then must be collected and sent to the server infrastructure (D2S). That server infrastructure has to share device data (S2S), possibly providing it back to devices, to analysis programs, or to people. From 30,000 feet, the protocols can be described in this framework as:

- MQTT: a protocol for collecting device data and communicating it to servers (D2S)
- XMPP: a protocol best for connecting devices to people, a special case of the D2S pattern, since people are connected to the servers.
- DDS: a fast bus for integrating intelligent machines (D2D).
- AMQP: a queuing system designed to connect servers to each other (S2S)

Each of these protocols is widely adopted. There are at least 10 implementations of each. Confusion is understandable because the high-level positioning is similar. In fact, all four claim to be real-time publish-subscribe IoT protocols that can connect thousands of devices. And it's true, depending on how you define "real time," "things," and "devices."

Nonetheless, they are very different indeed! Today's Internet supports hundreds of protocols. The IoT will support hundreds more. It's important to understand the class of use that each of these important protocols addresses.

The simple taxonomy in Figure 2 frames the basic protocol use cases. Of course, it's not really that simple. For instance, the "control plane" represents some of the complexity in controlling and managing all these connections. Many protocols cooperate in this region.

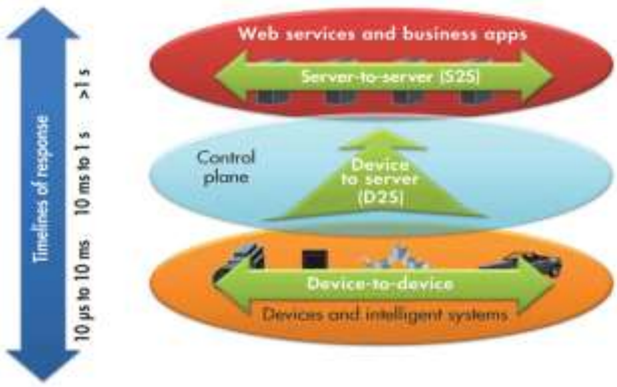


Fig 2. IOT Protocols Need to Address Response Time.

mqtt

MQTT, the Message Queue Telemetry Transport, targets device data collection *(Fig. 3)*. As its name states, its main purpose is telemetry or remote monitoring. Its goal is to collect data from many devices and transport that data to the IT infrastructure. It targets large networks of small devices that need to be monitored or controlled from the cloud.

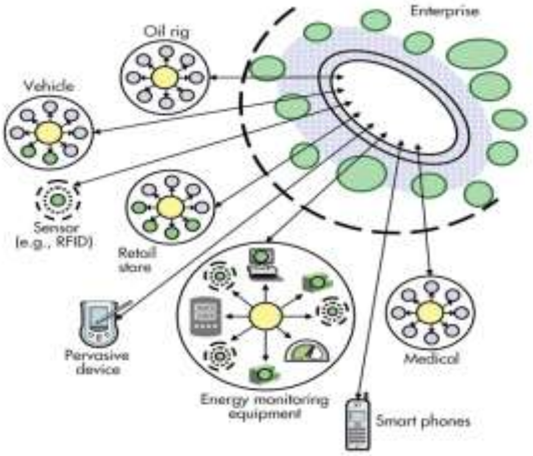


Fig 3. Message Queue Telemetry Transport (MQTT) implements a hub-and-spoke system.

MQTT makes little attempt to enable device-to-device transfer, nor to “fan out” the data to many recipients. Since it has a clear, compelling single application, MQTT is simple, offering few control options. It also doesn’t need to be particularly fast. In this context, “real-time” is typically measured in seconds.

A hub-and-spoke architecture is natural for MQTT. All the devices connect to a data concentrator server, like IBM’s new Message Sight appliance. You don’t want to lose data, so the protocol works on top of TCP, which provides a simple, reliable stream. Since the IT infrastructure uses the data, the entire system is designed to easily transport data into enterprise technologies like Active MQ and enterprise service buses (ESBs).

MQTT enables applications like monitoring a huge oil pipeline for leaks or vandalism. Those thousands of sensors must be concentrated into a single location for analysis. When the system finds a problem, it can take action to correct that problem. Other applications for MQTT include power usage monitoring, lighting control, and even intelligent gardening. They share a need for collecting data from many sources and making it available to the IT infrastructure.

XMPP

XMPP was originally called “Jabber.” It was developed for instant messaging (IM) to connect people to other people via text messages *(Fig. 4)*. XMPP stands for Extensible Messaging and Presence Protocol. Again, the name belies the targeted use: presence, meaning people are intimately involved.

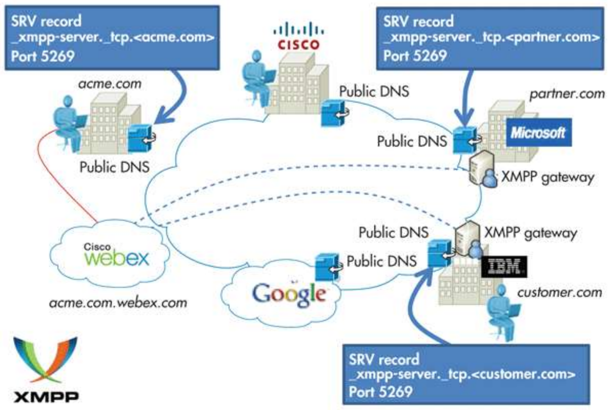


Fig 4. The Extensible Messaging and Presence Protocol (XMPP) Provides Text Communication between Points.

XMPP uses the XML text format as its native type, making person-to-person communications natural. Like MQTT, it runs over TCP, or perhaps over HTTP on top of TCP. Its key strength is a name@domain.com addressing scheme that helps connect the needles in the huge Internet haystack.

In the IoT context, XMPP offers an easy way to address a device. This is especially handy if that data is going between distant, mostly unrelated points, just like the person-to-person case. It’s not designed to be fast. In fact, most implementations use polling or checking for updates only on demand. A protocol called BOSH (Bidirectional-streams over Synchronous HTTP) lets severs push messages. But “real time” to XMPP is on human scales, measured in seconds.

XMPP provides a great way, for instance, to connect your home thermostat to a Web server so you can access it from your phone. Its strengths in addressing, security, and scalability make it ideal for consumer-oriented IoT applications.

DDS

In contrast to MQTT and XMPP, the Data Distribution Service (DDS) targets devices that directly use device data. It distributes data to other devices (Fig. 5). While interfacing with the IT infrastructure is supported, DDS’s main purpose is to connect devices to other devices. It is a data-centric middleware standard with roots in high-performance defense, industrial, and embedded applications. DDS can efficiently deliver millions of messages per second to many simultaneous receivers.

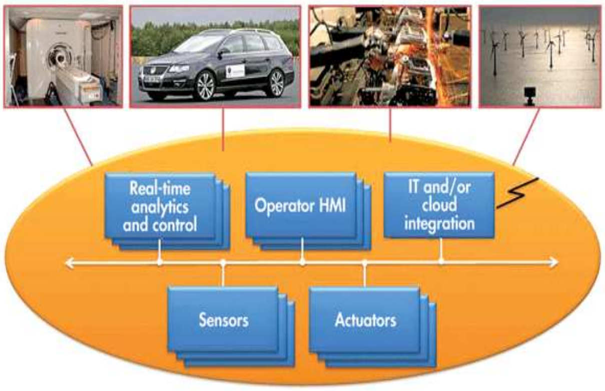


Fig 5. Data Distribution Service (DDS) Implements a Publish/Subscribe Architecture.

Devices demand data very differently than the IT infrastructure demands data. First, devices are fast. “Real time” is often measured in microseconds. Devices need to communicate with many other devices in complex ways, so TCP’s simple and reliable point-to-point streams are far too restrictive. Instead, DDS offers detailed quality-of-service (QoS) control, multicast, configurable reliability, and pervasive redundancy. In addition, fan-out is a key strength. DDS offers powerful ways to filter and select exactly which data goes where, and “where” can be thousands of simultaneous destinations. Some devices are small, so there are lightweight versions of DDS that run in constrained environments.

Hub-and-spoke is completely inappropriate for device data to use. Rather, DDS implements direct device-to-device “bus” communication with a relational data model. RTI calls this a “Data Bus” because it is the networking analog to a database. Similar to the way a database controls access to stored data, a data bus controls data access and updates by many simultaneous users. This is exactly what many high-performance devices need to work together as a single system.

High-performance integrated device systems use DDS. It is the only technology that delivers the flexibility, reliability, and speed necessary to build complex, real-time applications. Applications include military systems, wind farms, hospital integration, medical imaging, asset-tracking systems, and automotive test and safety. DDS connects devices together into working, distributed applications at physics speeds.

AMQP

Finally, the Advanced Message Queuing Protocol (AMQP) is sometimes considered an IoT protocol. AMQP is all about queues *(Fig. 6)*. It sends transactional messages between servers. As a message-centric middleware that arose from the banking industry, it can process thousands of reliable queued transactions.

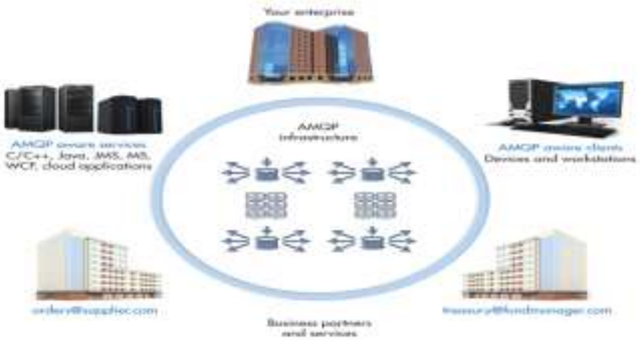


Fig 6. The Advanced Message Queuing Protocol (AMQP) is Messages-centric Middleware that arose from the Banking industry.

AMQP is focused on not losing messages. Communications from the publishers to exchanges and from queues to subscribers use TCP, which provides the strictly reliable point-to-point connection. Further, endpoints must acknowledge acceptance of each message. The standard also describes an optional transaction mode with a formal multiphase commit sequence. True to its origins in the banking industry, AMQP middleware focuses on tracking all messages and ensuring each is delivered as intended, regardless of failures or reboots.

AMQP is mostly used for business messaging. It usually defines "devices" as mobile handsets communicating with back-office data centers. In the IoT context, AMQP is most appropriate for the control plane or server-based analysis functions.

The Bottom Line

The IoT needs many protocols. The four outlined here differ markedly. Perhaps it's easiest to categorize them along a few key dimensions: QoS, addressing, and application.

QoS control is a much better metric than the overloaded "real-time" term. QoS control refers to the flexibility of data delivery. A system with complex QoS control may be harder to understand and program, but it can build much more demanding applications.

For example, consider the reliability QoS. Most protocols run on top of TCP, which delivers strict, simple reliability. Every byte put into the pipe must be delivered to the other end, even if it takes many retries. This is simple and handles many common cases, but it doesn't allow timing control. TCP's single-lane traffic backs up if there's a slow consumer.

Because it targets device-to-device communications, DDS differs markedly from the other protocols in QoS control. In addition to reliability, DDS offers QoS control of "liveliness" (when you discover problems), resource usage, discovery, and even timing.

Next, finding the data needle in the huge IoT haystack is a fundamental challenge. XMPP shines here for "single item" discovery. Its "user@domain" addressing leverages the Internet's well-established conventions. However, XMPP doesn't easily handle large data sets connected to one server. With its collection-to-a-server design, MQTT handles that case well. If you can connect to the server, you're on the network. AMQP queues act similarly to servers, but for S2S systems. Again, DDS is an outlier. Instead of a server, it uses a background "discovery" protocol that automatically finds data. DDS systems are typically more contained. Discovery across the wide-area network (WAN) or huge device sets requires special consideration.

Perhaps the most critical distinction comes down to the intended applications. Inter-device data use is a fundamentally different use case from device data collection. For example, turning on your light switch (best for XMPP) is worlds apart from generating that power (DDS), monitoring the transmission lines (MQTT), or analyzing the power usage back at the data center (AMQP).

Of course, there is overlap. For instance, DDS can serve and receive data from the cloud, and MQTT can send information back out to devices. Nonetheless, the fundamental goals of all four protocols differ, the architectures differ, and the capabilities differ.

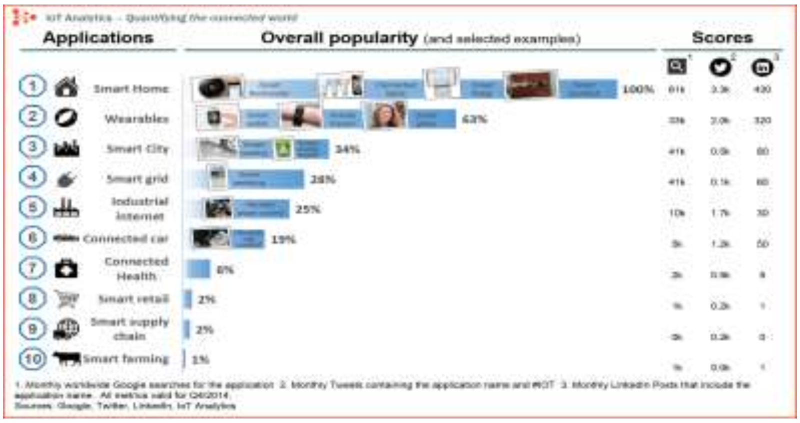
All of these protocols are critical to the (rapid) evolution of the IoT. The Internet of Things is a big place, with room for many protocols. Choose the one for your application carefully and without prejudice of what you k now.

VI. APPLICATION OF IOT

1. Internet of things examples extends from smart connected homes to wearables to healthcare. It is not wrong to suggest that IoT is now becoming part of every aspect of our lives. Not only internet of things applications are enhancing the comforts of our lives but also it giving us more control by simplifying routine work life and personal tasks.

2. With the recent hype about the future prospects of IoT has forced companies to take the initiative of coming up with basic building blocks of the internet of things i.e. hardware, software and support to enable developers to deploy applications that can connect anything within the scope of the internet of things.

3. We know that the potential of IoT markets is huge but there are some domains that will mature much faster than the rest. Here we list the application areas for the internet of things with examples that have the potential of exponential growth.



CONCLUSION

The World has been changed completely due to the Internet and Internet-based application development. Interaction in all scenario becomes seems impossible without it. IoT has potential to broaden its horizon by enabling communication between smart objects. IoT will change everything drastically if implemented successfully, But still, there are various issues which need thorough research to improve the quality of life. In this Paper, we have discussed various technologies with its specification that can result in making IoT a reality. In next section, we presented some handsome application of IoT and its comfort in life. Finally, some important issues that needed to be resolved have been discussed before wide acceptance of this technology. We finally conclude the need for new "smart" autonomic management, data aggregation, and protocol adaptation supporting trusted and authenticated communication between IoT objects is a key of successful and wide deployment of services provided over IoT. In this paper, a survey of IoT authentication techniques has been conducted to help other researchers in their classification and comparison. The classification has been done based on the inherent features of this authentication technique such as being distributed vs. centralized, flat vs. hierarchical. One can notice, although they show considerable potentials, that little research has been conducted which adopts hierarchical and distributed solutions. Most of these techniques require pre-registration step of a single authentication process since multiple authentication steps could result in further complication of the authentication protocol. Authentication techniques are divided between single and multiple credentials while concentrating on mutual authentication and being far from using special hardware. A comparison between these techniques according to the used evaluation models shows that most of them have used theoretical evaluation, and/or performance analysis in contrast to an implementation, or simulation approaches used by little others. In regards to security attacks, we can notice that little attention has been paid toward timing, forgery, denial of service and stolen smart card attacks. In summary, we recommend that future research may focus on hierarchical and distributed approaches that consider timing, forgery, denial of service, and stolen smart card attacks in their solutions. In this survey, we discussed and learned about IoT vision and services, technologies. Finally, we have great knowledge about the IoT services and communications among the network objects. In the proposed solution, we will provide the security to the IoT data and to avoid the security threats in the IoT network objects.

REFERENCES

[1]. Sajjad Hussain Shah, Ilyas Yaqoob "2016 the 4th IEEE International Conference on Smart Energy Grid Engineering"

[2]. Maha Saadeh1, Azzam Sleit2, Mohammed Qatawneh3, Wesam Almobaideen4"2016 Cybersecurity and Cyber forensics Conference", pp. 1-7

[3] Ms. M. Joharan Beevi,"A FAIR SURVEY ON INTERNET OFTHINGS (IoT)" Website References

[4] internetofthingswiki.com/iot-applications-examples/541/

[5] http://electronicdesign.com/iot/understanding-protocols-behind-internet-things

[6] www.globalresearch.com