International Journal of Engineering &Technology, 7 (3.12) (2018) 255-259

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Internet of Things: a Survey of the Advancements

Dhivya V[1], Apoorva Kumar Singh[2]

[1]*Assistant Professor, Department of Computer Science and Engineering, Sir M. Visvesvaraya Institute of Technology, Bengaluru*
[2]*UG student, Sir M. Visvesvaraya Institute of Technology, Bengaluru*
**Corresponding Author Email: [1]dhivya_cs@sirmvit.edu, [2]apoorva.singh157@gmail.com*

Abstract

Internet of Things is a very broad concept and it is the name given to the interconnection of everyday devices to simplify, ease or provide useful information to the user. The International Telecommunication Union (ITU) defines IoT as "A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies". The name "Internet of Things" was first coined in 1999 by Kevin Ashton in a presentation to Proctor and Gamble. In this paper, we review the protocols, architecture, and applications surfacing in the region of the Internet of Things in the current years. The web of things has the capability of changing a great part of the world we live in. IoT comprises of an advanced cluster of sensors inserted into various "things" that ceaselessly transmits and shares significant information to different gadgets and cloud. Information that causes us better see how these things function and cooperate. But how all of this can happen on such a large scale with so many devices transmitting data? A simple answer to that would be the Internet of Things platform that brings diverse information and provides a common language for the devices and apps to communicate with each other.

Index Terms: *Internet of Things, social IoT, Fog Computing, cloud computing, networks, sensors.*

1. Introduction

When Internet of Things started off in the year 1999 at MIT's AutoID lab. For completion of the vision of the project, major technological improvements were required. Questions like, how would we connect everything on the planet? Which wireless communication device would be used? How will the resultant data be processed? What developments should be made so that these technologies can become more economical and widespread.

In today's world much of these problems have been solved with plethora of alternatives to choose from. The cost of wireless radios, silicon chips, electronic equipment and cloud computers have dropped significantly. Access to a better and more reliable network is available. With all these technologies in place, a large number of IoT devices have started to appear in the market. A prediction was made by Cisco Internet of Things Group (IOTG) that there will be over 50 billion connected devices by 2020.

There are significant advancements that are being made in the intangible technologies relating to IoT like, routing protocols, cloud computing, analytics, network transmission protocols, scheduling algorithms etc. Due availability of scarce energy supply and unreliable network connectivity, it has become imperative to design IoT systems that are optimized for power usage. Scheduling algorithms are a fundamental piece for WSNs and IoT systems.

These algorithms enable us to choose which process to run and which message ought to have a higher priority than others. A study suggests scheduling of messages at cluster head nodes. Long Hop (LH) first is another algorithm that gives a higher priority to the information that is originating from far away devices and has hoped through a number of devices to reach its destination. The implementation results of this algorithm demonstrate that it cuts down in power consumption by 56% and the network throughput is increased by 62.50%. Along with that, it limits packet loss, transmission distance, and packet delays. The outcomes have been contrasted with some of the similar algorithms like first-come-first-serve (FCFS) and nearest job next (NJN). There are other algorithms as well that can be used for scheduling message based on the implementation conditions like Time Synchronized Channel Hopping (TSCH), short time process (SPT) algorithm etc.

The present state of IoT can be gauged with the help of Gartner's Hype Cycle, IoT is in the peak of inflated expectations area. A Hype Cycle is used to track the emergence, adoption, maturity of technologies. It has been estimated that IoT will take another 2 to 5 years to thrive in the market.

2. Architectures

A. Introduction

Because of lack of standardization, there is no single model that is used for engineering for IoT. Having a different architecture for different applications has its pros and cons. Various models have

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

been proposed by different scientists. Some of the architectures that we'll briefly look into are:

1) Three-layer Architecture
2) Five-layer Architecture
3) Cloud and Fog Architecture
4) Social IoT

B. Three Layer Architecture

Due to the simple design of this architecture this a commonly accepted high-level design. It consists of three layers: Perception layer, Network layer, and Application layer.

1) Perception Layer – The main task of the perception layer is to perceive the internal state of the object and the environment around it. It is the physical layer responsible for gathering valuable raw data from sensors and other smart objects. Several sensing technologies are used in this layer (e.g. GPS, IR, RFID, WSN, Gyro, etc.). This layer converts the physical values into digital signals making it convenient for network transmission.

2) Network Layer – The work of this layer is to connect all the smart things, gateways, network devices, and servers together and facilitate the processing of the perceived data from the perception layer. This layer is also used for transmitting information to the application layer with the help of various technologies (e.g. Zigbee, Bluetooth, Wi-Fi, infrared technology etc.). A middleware is employed here to process the massive amounts of data that is being generated. To realize this goal, cloud computing is the primary technology used in this layer which provides a suitable interface for storing and processing the data.

3) Application Layer – The data that is collected from the previous layer is used to draw inferences and get meaningful insights into the smart objects that are being monitored. This is the front end of the entire IoT structure and provides the required tools and services to actuate the environment. A wide range of impressive applications can be developed on this platform and made accessible to the user.

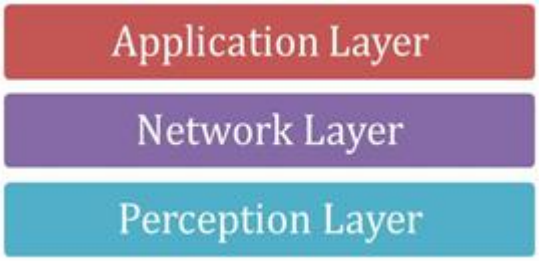

Fig. 2: Three-layer Architecture

C. Five Layer Architecture

For research on the finer aspects of the Internet of Things architecture, the researchers devised a new architecture which consists of five layers. The added layers are transport layer, processing layer, and the business layer rest all the layers are same as it was in the three-layer architecture. The work of the other three layers remains the same as was in the previous architecture. The work of the newly added two layers are:

1) *Transport Layer* **–** Transports the information from the sensor layer to the processing layer with the assistance of technologies like Bluetooth, Zigbee and so on.

2) *Processing Layer* **–** The work of this layer is to process the raw data coming in from the transport layer. It makes use of various technologies like cloud computing and big data.

3) *Business Layer* **–** It manages the entire IoT system.



Fig. 3: Five-layer Architecture

D. Cloud and Fog Architecture

Cloud computing predominantly focuses on centralized storage and processing of the data that is continuously being generated by the smart objects. In this type of a system, the cloud is at the center of the entire system. The reason for the dominance of a cloud model is because of the scalability, flexibility, plethora of visualization, storage, and analysis tools that are made available to the developer by the cloud platform.

Recently, there has been a move towards another system architecture namely, fog computing. What this basically does is process the time-sensitive data on the edge of the network itself, i.e. closest to where the data is being generated so that appropriate actions can be taken in time. Some key features of this model are:

1) Minimize latency
2) Conserve network bandwidth
3) Resolves the data privacy and security issue
4) Increase reliability

The features of this model practically have a wide range of applications ranging from industry to common households. An example where this type of technology can help common household is on house fires. A smart smoke alarm or fire alarm fitted in the kitchen can quickly send the data to the nearest edge server for taking appropriate action like turning off the gas stove or pumping water through the emergency water sprinkler. In this situation we cannot afford to wait for a response from the cloud to turn off the knob, the decisions need to be made as soon as possible. This is what makes the fog architecture an interesting model. The fog extends the cloud and brings it closer to the objects so that it can better act on the IoT data.

E. Social IoT

The intersection of IoT and social networking gave birth to this new paradigm of Social IoT. In this, services can be shared by the user to other users or other smart devices. Some features that can be offered by this kind of architecture are:

1) The SIoT structure offers great flexibility when it comes to designing the networks navigability so that the object and services can find each other effectively
2) A measure of trustworthiness can be developed for leveraging the degree of interaction among things
3) Models that are designed to study for Social Networks can be re-used to address the issues related to IoT

The kind of relationship that this model defines are:

1) Parental object relationship
2) Co-location object relationship
3) Co-work object relationship
4) Ownership object relationship

5) Social Object Relationship

We would like to conclude this section with a chart that best illustrates the use of different components at different layers of the IoT system.

3. Sensors and Actuators

The point of data generation are the sensors which collect data from the environment. These IoT sensors need to be small in size, consume the least amount of power and should have a low cost. They are also constrained by many working parameters like battery capacity, dependability, ease of deployment and accuracy.

1) *Mobile Phone based sensors* – Mobile phones have become ubiquitous devices. And these phones have many types of sensors embedded in it, along with processing power, storage and network connectivity for transmitting data to the cloud. Nowadays many applications are being built leveraging the data produced by the sensors and using them to produce meaningful results. Some sensors with which the mobile phones are shipped with are accelerometers, gyroscope, camera, microphone, magnetometer, GPS (Global Positioning System), light sensor and proximity sensor. Some smartphones manufactured by Samsung even have a thermometer, barometer, humidity sensor and heartbeat sensor built in the phones. One of the application that was developed that made use of the smartphone sensors was an activity recognition application [3].

2) *Medical Sensors* – Examples of these type of sensors are heart rate sensors, pulse sensors, sensors for estimating pulse, body temperature, breath rate and blood glucose levels and so forth. These sensors can be set on the individual's body which will then send the information to the cloud where it can be seen by the specialist and relatives of the individual.

The information being gathered here is context dependent i.e. it should be merged with other logical data, for example, physical movement. For instance, our breathing rate escalates when we work out. If only breathing rate is considered, we cannot deduce breathing related issues. Therefore the data needs to be combined with other data to make more appropriate inferences.

3) *Neural Sensors* – Brain signals can be read with the help of a device called an EEG (Electroencephalography). The neurons communicate inside our brains because of the flow of charged Sodium and Potassium ions. The electric field generated due to the firing of a neuron can be measured on the scalp with the help of special sensors. The value from these sensors can be used to control the actuators or can be used to have a better mental wellbeing.

4) *Chemical Sensors* – The electronic nose (e-nose) and electronic tongue (e-tongue) are devices that can be utilized to detect chemicals based on their smell and taste. These devices accompany a variety of sensors combined with an advanced pattern recognition to identify the stimulus. These devices can be used for testing food items, and in smart kitchens etc.

5) *Radio Frequency Identification (RFID)* – It is an identification innovation in which an RFID label conveys the information. What's more, is that the information is perused by the RFID reader. The label exchanges the information put away in it with the assistance of radio waves. It doesn't require a viewable pathway like QR code. The range of this device varies with frequency and can go up to hundreds of meters. There are two types of RFID tags: passive and active. Passive tags draw the power from the EM waves emitted by the reader to transmit the data. Whereas the active tag makes use of an active power supply to transmit the information.

6) *Actuators* – These are devices which convert electrical energy supplied to them into useful energy for effecting a change in the environment. Examples of these kinds of devices are light bulbs, motors, automatic door locks etc.

4. Preprocessing

We need to analyze, process and store the huge amounts of data that is being generated. The most common answer to this problem is the use of cloud platforms that offer these services. But sometimes some IoT application require the processing of data to take place on the edge of the network. Still, there are challenges that we face when it comes to using these cloud platforms.

1) *Mobility* – A large portion of the devices and the objects would be motile which makes it difficult for them to speak with the cloud

2) *Reliability* – Applications where real-time processing of data is required and time is critical. Cloud-based applications have a bit of latency attached to them because of the staggering amounts of requests that the cloud has to manage from all the other smart devices. Network connectivity also plays a major role here as it contributes to network latency.

3) *Power Constraint* – A continuous communication cannot be done with the cloud as the IoT devices are battery powered and communication consumes a lot of power.

These problems can be solved with the help of a concept called as fog computing. In this, some compute and storage resources are brought to the edge of the network instead of relying on the cloud for everything. These edge computers provide us with the capability of local processing, sorting, and analyzing data before sending the data to the cloud servers. The Fog and Cloud paradigm both compliment each other by overcoming the demerits of each other. Features that will be provided by fog computing are:

1) Lower Latency
2) Lower bandwidth consumption
3) Real time interaction
4) Increased reliability

5. Communication

One of the core components of a smart object is its ability to communicate with other objects and devices. Still, there are various challenges that we need to tackle before moving on, some of them are:

1) *Identification* – Identification of devices on the network in the midst of thousands of other devices

2) *Low Power communication* – Since these devices will be battery powered so power spent in communication plays a key role here.

3) *Better routing of data* – In case of a multi-hop system where the data from the sensor reaches the network gateway through multiple hops from other devices. A good, low resource consuming routing protocol needs to be developed for IoT.

Generally, the smart devices connect to the Internet via the IP stack. This stack consumes a lot of power and resources from the connecting device and hence is not a suitable method for connecting to the internet. Other ways have been proposed to tackle this problem one of which is the by the using non-IP networks to connect to a gateway which connects to the internet using an IP stack. These non-IP networks can make use of NFC, Bluetooth technology, Zigbee etc. In this section we'll be briefly looking into various communication technologies that can be used in IoT:

1) *Near Field Communication (NFC)* – It is a very short range communication technology which works at a distance of few centimeters only. It can operate in two modes: active and passive. Passive mode is particularly useful in devices that have limited power. One noticeable feature of NFC is its ability to have a two-way communication.

2) *Wireless Sensor Networks (WSN)* – When a large area needs to be monitored with the help of a large number of sensors deployed at diverse locations, we use Wireless Sensor Networks. It overcomes the shortcomings of non-IP based communication technologies like Bluetooth. These sensor networks first send the data to the gateway which then forwards it to the cloud server.

3) *Bluetooth Low Energy (BLE)* – This was developed by Bluetooth Special Interest Group for use in power constrained devices. This technology is not compatible with classical Bluetooth but has a similar protocol stack. Also, BLE does not support streaming of data. The BLE protocol stack also has the support for IP based communication along with an expected data rate of 1 Mbps.

4) *Low Power Wi-Fi* – The WiFi alliance has recently developed WiFi HaLow. It devours bring down power consumption than conventional WiFi and furthermore has a greater range. It has a support for IP connectivity and was developed to deal with the communication problem in the wireless sensor networks (WSN). These devices operate in the sub-gigahertz band of 900 MHz. At the same output power, lower frequencies will travel farther than higher frequencies. We'll get a lower speed than what we might expect in higher bands (2.4 & 5GHz) but the connection would be more stable because of its farther reach.

5) *Zigbee* – Produced by Zigbee Alliance which works for low cost, low energy communication technology. It is built upon the IEEE 802.15.4 standard. This has the capability of multihop routing. The range of these devices are very small (10-100 meters).

6. Middleware

For developing applications that can easily make use of the data generated by the sensors we need an abstraction layer that takes care of the interoperability of heterogeneous devices. It abstracts the hardware and provides a suitable interface for communication, data management and computation for the developer. Problems that are solved by IoT middleware are:

1) *Programming abstraction* – Facilitates the exchange of information between heterogeneous devices

2) *Device management* – This enables other devices to be discovered on the network and announce their presence. The middleware will give an APIs to list the IoT gadgets, the services offered, and their capacities, the activity they can perform, or the state in which they can be in. etc.

3) *Scalability* – Middleware provides the right infrastructure for allowing a large number of devices to communicate with the cloud. It also has load balancers for balancing a large number of requests simultaneously.

4) *Cloud Services* – These cloud platforms provide tools to analyze, store and process big data produced by smart objects and devices and apply machine learning algorithms to predict certain values. Due to the numerous tools provided by these platforms, possibilities are endless of what can be developed. The Some examples of middlewares are Oracle's Fusion Middleware, Open IoT, MiddleWhere, Hydra, Aura, TinyDB, WiseMID etc. The middleware layer can be further divided into multiple layers:

1) Interface Protocols – This part is accountable for giving technical interoperability. Here interoperability implies the capacity of two different devices running on different frameworks to interoperate by utilizing same communication protocols.

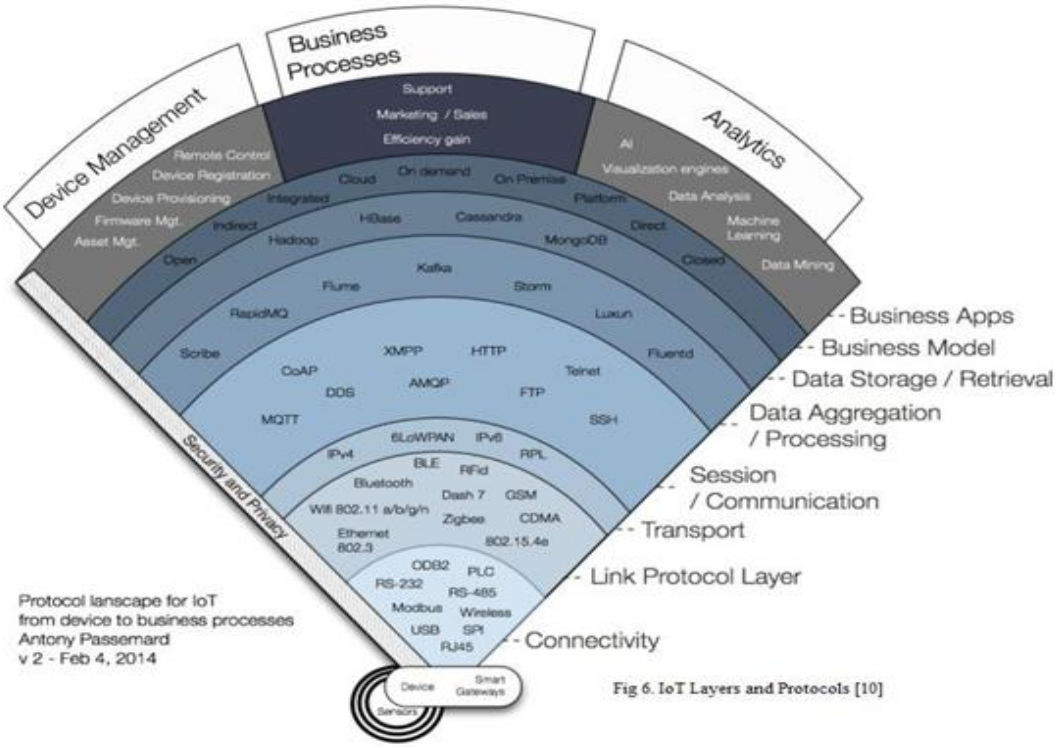

Fig. 6: IoT Layres and Protocols [10]

2) *Device Abstraction* – This part is in charge of giving an abstract format to engineers to help and ease the interaction of the application components with low-level devices.
3) *Central control and Management* – Responsible for supporting context-aware computation.
4) *Application Abstraction* – A restful API or query-based language may be provided for a high-level interface to interact with the smart objects and devices.

Middlewares can also be classified on the basis of their designs.

1) *Event-Based* – All the components in this system interact with each other with the help of events. Ever entity could subscribe to certain types of events and get notified of those specific type of events. These events are generated by what is called as publishers and are consumed by consumers.
2) *Service-oriented* – This middleware is based on something called as Service Oriented Architectures (SOA). In this, each module provides its services through appropriate accessible interfaces. All the services offered by providers are present in a location called as service repository, where all consumers can discover and bind to the required services.
3) *Database Oriented* – In this model, the system of IoT devices is considered as a relational database framework that can be questioned by the developer's application with the help of a query language.
4) *Semantic* – This gives us a framework to talk to different types of devices which communicate uniquely using different protocols. This particularly eases the work that the application developer has to do when interfacing with heterogeneous devices.
5) *Application Specific* – This is a custom built architecture to support a specific type of IoT infrastructure. In this, the application and the middleware are closely related and does not offer any general purpose solution and is tailored to solve the problem at hand.

7. Conclusion

Fig 6 summarizes all the different layers that are present in an IoT infrastructure along with all the major tools, protocols and services that work at different layers. We didn't discuss any of the applications of IoT because all the readers might already be aware of the places this technology can be employed to benefit the lives of millions of people. Still, this technology is in its nascent stage and will continue to grow at an unprecedented rate over the years to come. People are still skeptical about sharing the data related to their everyday life all the time to cloud computers for processing, worrying about data leaks and other hacks. This field has a huge potential to impact human lives in numerous ways over the next decade.

References

[1] A. Anjum and M. U. Ilyas, "Activity recognition using smartphone sensors," in Proceedings of the IEEE 10th Consumer Communications and Networking Conference (CCNC '13), pp. 914– 919, Las Vegas, Nev, USA, January, 2013.

[2] Atzori, L., Iera, A., Morabito, G., Nitti, M.: The social internet of things (siot) when social networks meet the internet of things: Concept, architecture and network characterization. Computer Networks, Volume 56, Issue 16, 3594 – 3608, (November 2012).

[3] Conti, Mauro, Ali Dehghantanha, Katrin Franke, and Steve Watson. "Internet of Things security and forensics: Challenges and opportunities.": 544-546, (2018).

[4] Gartner identifies three megatrends that will drive digital business into the next decade report for 2017, Gartner Inc., https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/

[5] Hu, P. (2015, October). A system architecture for software-defined industrial Internet of Things. In Ubiquitous Wireless Broadband (ICUWB), 2015 IEEE International Conference on (pp. 1-5). IEEE.

[6] L. Farhan, L. Alzubaidi, M. Abdulsalam, A. J. Abboud, M. Hammoudeh and R. Kharel, "An efficient data packet scheduling scheme for Internet of Things networks," 2018 1st International Scientific Conference of Engineering Sciences - 3rd Scientific Conference of Engineering Science (ISCES), DIYALA, Iraq, pp. 1-6, 2018.

[7] Navani, D., Jain, S., & Nehra, M. S. (2017, December). The Internet of Things (IoT): A Study of Architectural Elements. In Signal-Image Technology & Internet-Based Systems (SITIS), 2017 13th International Conference on (pp. 473-478). IEEE.

[8] Pallavi Sethi and Smruti R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," Journal of Electrical and Computer Engineering, vol. 2017, Article ID 9324035, 25 pages, doi:10.1155/2017/9324035, 2017.

[9] Romdhani, Imed & Abdmeziem, Riad & Tandjaoui, D. (2015). Architecting the Internet of Things: State of the Art.

[10] The Internet of Things Protocol stack – from sensors to business value. https://entrepreneurshiptalk.wordpress.com/2014/01/29/the-internet-of-thing-protocol-stack-from-sensors-to-business-value/