IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 5, May 2016.
www.ijiset.com

ISSN 2348 – 7968

The Internet of Things: A survey of Technology, Security and Applications

Karan Patil[1] and Priyansh Bendre[2]

[1] Kendriya Vidyalaya, Pune, India

[2] University of Pune, India

Abstract

The Internet of Things involves analysis of data collected from everyday things (e.g Cars, Refrigerator, etc) containing individual sensors, which communicate over a network by sending data to the cloud via a gateway for further computation and reactions. To clarify the need of IoT its social benefits and currently available IoT technologies are introduced as well security concerns of IoT and methods to resolve them are discussed. Also terminologies regarding networking and machine communication are attended.

Keywords: *Internet of things, IoT, Ambient Systems, Connected System, Future Technology*

1. Introduction

Over the last few years, the internet has been in a constant state of evolution. Internet has changed immensely from being just a medium for viewing and publishing data, to a two way active communication channel. This active communication channel, AKA Web 2.0, has transformed the way people connect and transfer data. From sharing crucial information to a casual interaction over the social media, the Web 2.0 has come a long way. This data analysed from the human interaction with and over the internet has led us to a point where we as a human, using the data from the internet, are able to make well informed and better targeted decisions. This has brought a paradigm shift in controlling and implementing different decisions, which were not possible a few years ago. This decisions can be in the form of traffic congestion control, customisation or manufacturing control on the conveyor systems, medical assistance control and plethora of other situations.

We have travelled a great distance with our Sensor Networks. From NFC[1] to RFID[2], we have explored new territories of communicating with the system, minimising human interaction and thus minimising human errors in the system. This idea of communication of a system gave rise to the a new concept, which was communication without human interaction with the system.

This idea of inter-communication, analysing and processing data within systems sans humans, is what led us to explore an uncharted sector of technology, which is

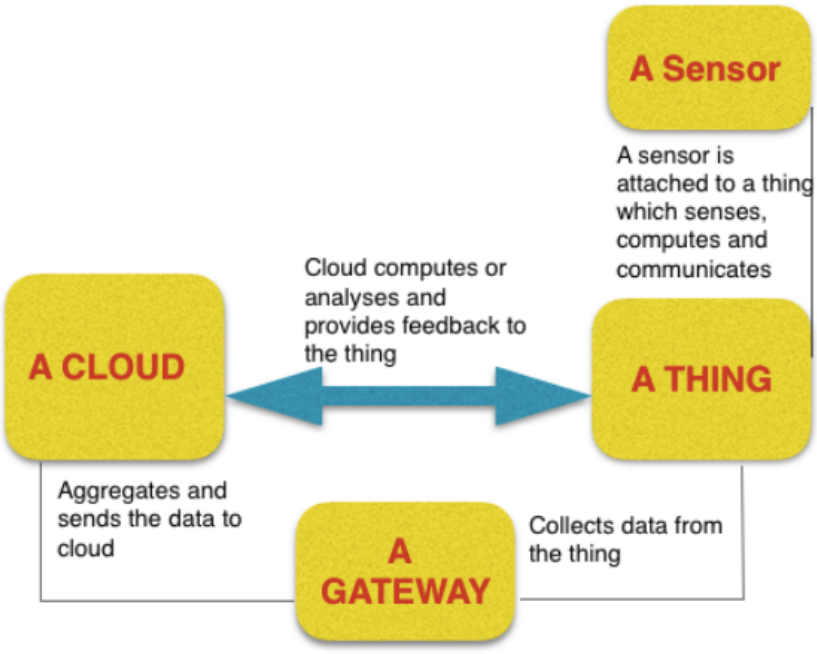

Fig. 1 Internet of Things - Working

ISSN 2348 – 7968

the Internet of Things (IoT). Though there is no universal definition of Internet of Things, we can simply describe it as "Internet of systems, which collect, process and exchange data to achieve some useful objective".

The concept of interaction between machines is not alien to us. It is the basic principle on which clients, servers and routers work. Though the basic idea may seem similar, IoT takes a whole different perspective towards the communication of the devices. IoT can include any basic device from a laptop, Mobile Phones, Vehicles to cameras, traffic signals, smoke detectors and anything and everything. By connecting these physical systems to a network, analysing and processing the data acquired from the systems, the systems can react to situations on its own. Ambient intelligence[3] has made work more efficient and productive for humans.

2. Survey Methodology

We went through the data aggregated from different sources and step by step worked upon it to deduce simplistic and much more precise information on the topic of Internet of Things.
We have gone through a range of Research and survey papers available in the libraries and on the internet. We aimed to better understand and distinguish IoT by going through the websites and papers like

- Google Scholar
- IEEE
- Wikipedia
- Elsevier Journal

We will be studying hardware software requirements, technology which work in tandem with IoT and security and other issues in detail.
We carefully and throughly studied 37 Papers compiled from various sources spread across national and International journals. We examined the details of these journals to analyse and pen down the concepts of Internet of Things to better understand and provide a better and easier perspective.

3. Technologies Involved

3.1 Hardware

When we think of IoT we are forced to think about various existing technology which are being used and how IoT is different than the existing technology or how we can use the existing technology resembling to connected systems and make IoT much more accessible and feasible for the mass market. The critical hardware infrastructure includes RFID, NFC and Sensor Networks. Building IoT Systems exclusive of these robust systems and not utilising there potentials would be a waste of resources.

RFID (Radio Frequency Identification) is a technology to identify and detect an object carrying an RFID Tag. An RFID tag is a device which typically can be produced in a very small form factor and can carry approximately 200 bytes of data. RFID are not a replacement for barcodes but in comparison work better than barcodes as they contain much more data and do not require line of sight (LOS) for detection. RFID is commonly being used in Transport, Manufacturing and Pet identification industry.

NFC (Near Field Communication) is communication protocol which enables two different devices (generally portable devices) to communicate (transfer data) from a very close distance. The distance practically required between two devices is found out to be less than 4 cm. As the small distance provides extra bit of security, NFC is being commonly now being used in payment systems. Many phones today support payment through NFC. Unlike RFID, NFC is a really short ranged identification and data exchange medium.

Sensor Networks are the group or system of the sensors working together for a particular goal to monitor any physical or environmental conditions. These sensors then pass the data retrieved through a network, to other sensors or the processors to analyse, process and react to the data accordingly. These sensor networks today are commonly used to measure temperature, sound, pressure, humidity etc.

3.1 Software

Cloud Interfaces are the most important aspect for Internet of Things as most of the data is being processed and stored on the cloud. As cloud storage is constantly in touch with the IoT device, Cloud interfaces should be feasible, durable and affordable for the masses.

Communication Standards vary with the networks connected or involved. To implement IoT and reap optimal benefits, the communication protocols and rules for exchange of data over the network should be in sync and comply international norms for data exchange and security.

Development is one of the major part of any technologies success. Many prototyping products like Arduino Uno, Arduino Mega, Intel Galileo, Raspberry pi and Beagle bone are in the market to better understand and prototyping the idea. A range of IDE's and Embedded OS are available on the internet which are required for the development and learning phase of the system.

4. IPv6

IPv6[4] is not just important but one of the necessities of IoT for long term success. Being a 32 bit protocol, IPv4 provides a shorter range of addresses. Because of the number of systems interacting today through internet, IPv4[5] is rapidly exhausting. This proves to be a big problem as the basic concept of IoT is to bring almost EVERYTHING online and connect it to the internet. IPv4's limitation of 32bit makes it able to

ISSN 2348 – 7968

support just approximately 4.2billion addresses. Which may look a lot but in real life will not be able to support even the bare minimum devices if the IoT concept holds true to it's current progress.

In contrast, IPv6 is a 128bit protocol. It is a major and much needed improvement over the IPv4 as it eliminates the first hurdle in the path of IoT due to the use of IPv4. Instead of supporting a dotted decimal system like in IPv4, IPv6 supports a hexadecimal system which helps it gain an exponential increase in number of addresses over IPv4. IPv6 is slowly but pacing up and the phase shift towards much bigger network is already underway.

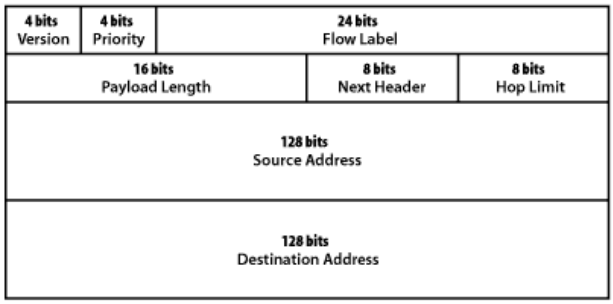

Fig.2 Packet format of IPv6[6]

World is adopting the IPv6 format slowly but steadily as still many routers and older switches do not support IPv6 format. And a sudden change is the format may put extra pressure on the existing infrastructure and may increase the cost of upgrades for many. The total adoption rate from the graph seems to be 12% as of now but is increasing at a good rate.

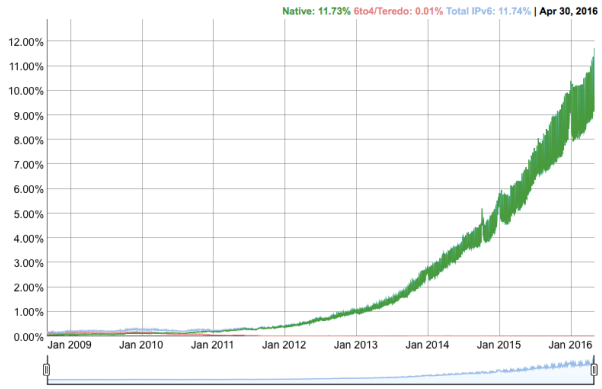

Fig.3 Total Adoption Rate [7]

In india IPv6 Adoption compared to the world is merely 0.76% [8].

5. Machine to Machine Communication

M2M refers to the machine to machine communication model may be wired or wireless in which two or more devices are connected directly to communicate between one another instead of any intermediate client server.

These machines use protocols like Bluetooth, Z-Wave, or ZigBee to establish direct machine-to-machine communications.[9]

This communication model is used mostly in home automation systems, which use small amount of data to be transferred at a typically lower data transfer rate.
Machine-to-machine communication protocols are not compatible, forcing the user to select a family of devices that employ a common protocol. For example, the family of devices using the Z-Wave protocol is not natively compatible with the ZigBee family of devices. [10]

M2M communication is an important aspect of warehouse management, remote control, robotics, traffic control, logistic services, supply chain management, fleet management and telemedicine. It forms the basis for the Internet of Things (IoT). [11]

With a potential market of probably 50 million connected devices, M2M offers tremendous opportunities as well as unique challenges. These devices vary from highly-mobile vehicles communicating in real-time, to immobile meter-reading appliances that send small amounts of data sporadically. [12]

6. Security and other concerns of IoT

The security of a network is an issue ever since the first two computers were connected to each other. The IoT has become unstoppable since its origin and the evolution has been accelerating high, eventually everything connected in IoT will be wireless. The major concern with the IoT is the risks and securities it faces. Broad scopes of risks and securities are considered as challenges in the IoT, however in this paper some major issues are addressed. The more IoT devices gets integrated in our life the more dependent we are. So when they go wrong, its much worse problem for us. Whether accidental or malicious, interference with the controls of a pacemaker, a car, or a nuclear reactor poses a threat to human life[13]. Below are the three key factors of safety in IoT discussed briefly.

6.1 Security Issues

IoT has the ability to automatically transfer data over a network. Security is paramount for the safe and reliable operation of IoT devices. The most important concern of the internet service is the how much it can be trusted with our data and behaviour in particular with the IoT devices. As user of internet services, applications and connected devices we need a high degree of trust over our interaction with it at the stake of the data being utilised with it and the activities we perform in relation to the internet. The security of IoT is linked with the ability of the user to trust their environment.[14] One of the top most priority of the IoT devices and service makers must be ensuring security in it.

ISSN 2348 – 7968

As the number of people connected with the internet services increases the vulnerability of the data being hijacked also increases efficiently. Towards the future outlook our efficiency to work without devices connected to the internet service would decrease effectively. Our exception is a completely secured interaction with these devices and services even after recognising the fact that no device can be absolutely secured all because of the fast evolving security implementations. For instance if your pacemaker is hacked or introduced with some worm it might result in death as well.

6.2 Risks Faced by IoT

The major risks handled by the IoT is the loss of data and malicious manipulation of data. The security concern of these devices is analogous to endless cat-and-mouse game in which new security threats evolve every time and accordingly manufacturers and service providers continuously respond to them. The risks of the IoT devices also depend on the user as, for some people it might not matter whether their refrigerator is sending spam emails to the world and might spend less money buying relatively cheaper machines which are poorly secured and are highly prone to malicious programs.

With your IoT devices you don't have depend on people much for your job to be done, you can depend on your IoT device to do things for you, as a result of which you don't have to deal much with people, so the downside here is that you become socially isolated. Another major downside of IoT is that you become more dependent on technology. For instance all our daily work nowadays is done on email, if email goes down for a particular day, its a problem, we communicate with people through emails work with them through emails, our work stops. Similarly in IoT if your network goes down or your device malfunctions its a problem for you because your dependent on it.

6.3 Privacy

The IoT devices are observing us, analysing our behaviour pattern most probably for our benefits. But they are observing us a lot, they become pervasive and happen to be omnipresent. For instance our cellphones GPS technology, in many phones its constantly on as many applications relay on the data being sent by it, but all our locations are also monitored to some central location may be they are using it for good purposes to help you but it is tracking you all the time and sending it on cloud server, and while installing the applications we often just accept the terms and conditions in the agreement which may transfer the ownership of our data to them and they might sell the data to some third party company. So its hard to keep track of our data as a user. Another way in which our data can be manipulated in a negative way is through hackers, our data is being stored in clouds which can be hacked by hackers and be used for ill purposes. Even encrypted data is decrypted in use.

6.4 Best Security practices to secure IoT

First and foremost is to secure your WiFi network connection, take control over the WiFi administration because all your IoT operations take place from your network connection. Make sure that all your online security updates are up to date.[15] Along side you should have privileged user control access over your network so that unknown users can be detected which might cause potential harm to the network followed by super user access over the connected devices. Another major responsibility of the consumer of IoT products is to stay updated with the latest security tweaks and features and try to modify the network accordingly is it suits the network and is more secured than the current methods. Its a common problem that people forget passwords or valid credentials to their network administration so it is suggested to always have a bypass emergency response system. Apart from network implementing good identity and access management program to the connected device is also of almost importance because the connected devices might also give access to the network administration, a good example of such a technology is the Cloud identity approach.[16] At the time of network installation quality layered authentication design must be ensured.

6.5 Types of Security

Encryption is the process of encoding our information in a format which could be decoded only by the authorised recipient. It does not prevent from interception but instead does not give out access to the data without a specified key. There must be end-to-end encryption or token based access control to protect the devices from fraudulent data transmission.

Physical Security - Another important security aspect of the IoT module is its physical security, which includes security against theft, adverse whether and environmental conditions as well as concerns regarding the physical being of devices. To protect the modules from theft proper measure should be taken while casing the module and the placement of the arrangement should be such that it would offer full security against the theft. Considering the environmental aspect the module should be properly tested according to the conditions in which it would be installed also it should be immune to the physical failures and proper recovery.

7. Applications

7.1 Social Benefits

IoT devices makes life easier in lot of different ways by answering many of our daily life questions like "what food do i need?", "which is the best hotel near my location" or "does my car needs servicing?". It helps industries become independent of people, by adding automation for simple things for which man force was required at wages higher than the maintenance cost of such devices, IoT handles things you need humans for.

ISSN 2348 – 7968

Broadly stating IoT devices help link to the world, as a circumstance of which global interaction with people is possible and information can be accessed conveniently without much hassle and faster than possible before. IoT enhances our interaction with people in different form with the growing wireless technology.

7.2 Implemented Technologies

There are already available IoT based technologies which unknowingly or knowingly we all have been using. Below are some of the IoT based technologies discussed briefly suggesting their features and areas of implementation:

LG Internet Digital DIOS[17] is a modern technology, based on IoT released in June 2000. The refrigerator's face is a TFT-LCD screen with TV functionality, other provisions included are a webcam as a scanner to track whats inside it and LAN connectivity. For the interaction with the refrigerator an electronic pen is used. Digital data memo, schedule management and video messaging are possible as well as the display showcases the status of the refrigerator such as freshness of food items, cooling temperature, recipes and nutrition of the food stored inside.

Augmented Maps are maps meant for tourists attached with tags that allow NFC-equipped phones to automatically call web service and receive data regarding local hotels, restaurants , monuments and events related to the area of interest for the user.

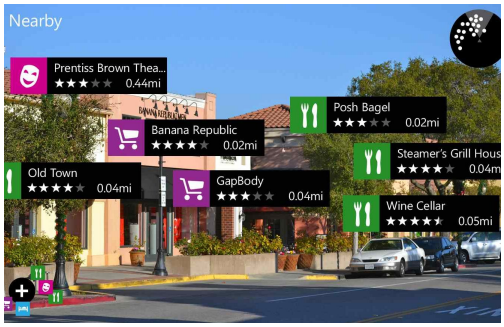

Fig. 4 Augmented Maps[18]

Prodigy Espresso[19] is smart coffee maker, a gadget designed to serve espresso stored in aluminium pods and ordered through cellphone. Its smart capabilities are made available via a mobile application, the user can brew coffee on demand or schedule beverage creation ahead of time. It is expected to communicate with smart phones and tablets using bluetooth wireless networking.

Xiaomi Yeelight[20] is a LED smart light bulb with brightness adjustment and remote control via wifi, which saves energy. The LED lamp operates at 100-220V, has luminous flux of 600 lumen, service life of 25000h and operates at 8W. The brightness of the lamp can be remotely adjusted using WiFi communication between the lamp and smart phone.

Fig. 5 IoT based LED Smart Bulb[21]

Foobot[22] is an air quality monitor, which is integrated with various sensors to track CO_2,CO,tVOC,PM2.5 , temperature and humidity stats. The stats are then sent to the smart phone or tablet connected to the same wireless network as the Foobot. Also the Foobot app along side collecting data from the device gives advice about best practices to ensure purer air inside the living space.

Amazon dash[*23*] is a single WiFi enabled button the serves one purpose, to order a single pre programmed item from Amazon. It attaches to any surface and upon pressing the button, with pre registered Amazon account an order is placed for that particular pre programmed item whenever you run out of it.

Fig. 6 IoT Smart Shopping Buttons[24]

8. Conclusion

Internet of Things though is in the early stage of it's lifespan but the amount of research and the number of advantages over the disadvantages show that the IoT will become much more integral part of our daily lives and make the lives of people easier.

9. References

[1] Near Field Communication "https://en.wikipedia.org/wiki/Near_field_communication"

[2] RFID "https://en.wikipedia.org/wiki/Radio-frequency_identification"

[3] Ambient Intelligence "https://en.wikipedia.org/wiki/Ambient_intelligence"

ISSN 2348 – 7968

[4] IPv6 “https://en.wikipedia.org/wiki/IPv6”

[5] IPv4 “https://en.wikipedia.org/wiki/IPv4”

[6] Packet Format image “http://www.techietek.com/wp-content/uploads/IPv6-packet-Format.png”

[7] IPv6 Adoption Rate “http://www.google.com/intl/en/ipv6/statistics.html”

[8] Adoption Rate in india “https://www.vyncke.org/ipv6status”

[9, 10, 14] Karen Rose, Scott Eldridge, Lyman Chapin, Internet Society, ”The Internet of Things: An Overview” , October 2015

[11] http://internetofthingsagenda.techtarget.com/definition/machine-to-machine-M2M

[12] http://tec.gov.in/pdf/Studypaper/White%20Paper%20on%20Machine-to-Machine%20(M2M)Communication.pdf

[13] “Security in the internet of things-Lessons from the past to connected future” Wind, January 2015

[15] “https://securityintelligence.com/events/securing-the-internet-of-things”

[16] “http://www.darkreading.com/identity-and-access-management/connect-a-modern-approach-to-mobile- cloud-identity/d/d-id/1113894”

[17] “https://en.wikipedia.org/wiki/Internet_Digital_DIOS"

[18] “https://az648995.vo.msecnd.net/devices/2013/01/Nokia-Lumia-920-City-Lens-Demo1.jpg”

[19] “https://www.nespresso.com/prodigio/experience/desktop/#/en/uk”

[20] “http://xiaomi-mi.com/mi-lighting/xiaomi-yeelight-led-smart-light-bulb”

[21] “http://des.gearbest.com/uploads/2015/201512/heditor/201512121736224010.jpg”

[22] “http://foobot.io"

[23] “https://en.wikipedia.org/wiki/Amazon_Dash"

[24] “http://amazondashbutton.info/wp-content/uploads/2016/02/amazon_dash_button.jpg”