International Journal of Engineering Studies and Technical Approach
IJESTA
ISSN No. 2395-0900

Internet of Things

Arpita R*, Karan Saxena & Amit Asish Bhadra*****

Students, Sir M. Visvesvaraya Institute of Technology

ABSTRACT:

This document contains basic information about Internet of Things (IoT), history which includes details about its various elements, applications, working as well as its advantages and disadvantages and the types of services (security)

Keywords: Internet of Things, Communication, Sensors, Network, Data, Frequency.

I. INTRODUCTION

Fig 1. Internet of Things

Kevin Ashton coined the phrase "Internet of Things" to describe a system where the Internet is connected to the physical world via 'ubiquitous sensors'.

The Internet of Things, also called The Internet of Objects, refers to a wireless network between objects, usually the network will be wireless and self-configuring, such as household appliances. "Internet of Things" has come to describe a number of technologies and research disciplines that enable the Internet to reach out into the real world of physical objects.

The following definition of IoT has been developed by Cisco Systems, Inc:

> *"The Internet of Things (IoT) is a computing concept that describes a future where everyday physical objects will be connected to the Internet and be able to identify themselves to other devices. The term is closely identified with RFID as the method of communication, although it also may include other sensor technologies, wireless technologies or QR codes."*

II. HISTORY

The concept of a network of smart devices was discussed as early as 1982, with a modified Coke machine at Carnegie Mellon University becoming the first internet-connected appliance, able to report its inventory and whether newly loaded drinks were cold. Mark

Weiser's seminal 1991 paper on ubiquitous computing, "The Computer of the 21st Century", as well as academic venues such as UbiComp and PerCom produced the contemporary vision of IoT.

The concept of the Internet of Things first became popular in 1999, through the Auto-ID Center at MIT and related market-analysis publications.

As of 2015, the vision of the Internet of Things has evolved due to a convergence of multiple technologies, ranging from wireless communication to the Internet and from embedded systems to micro-electromechanical systems (MEMS).

III. IoT ELEMENTS

There are three IoT components which enables seamless ubicomp:

- Hardware - made up of sensors, actuators and embedded communication hardware.
- Middleware - on demand storage and computing tools for data analytics.
- Presentation - novel easy to understand visualization and interpretation.

We discuss a few enabling technologies in these categories which will make up the three components stated above:

Radio Frequency Identification (RFID):RFID technology is a major breakthrough in embedded communication which enables design of microchips for wireless data communication. The applications can be found in transportation (replacement of tickets, registration stickers) and access control applications as well.

Wireless Sensor Networks (WSN): This is a sensor network consisting of a large number of intelligent sensors, enabling the collection, processing and analysis of valuable information, gathered in a variety of environments. Sensor data are shared among sensor nodes and sent to a distributed or centralized system for analytics.

Addressing Schemes: The ability to uniquely identify ‘Things’ is critical for the success of IoT. Every element that is already connected and those that are going to be connected, must be identified by their unique identification, location and functionalities.

Data Storage and Analytics: One of the most important outcomes of this emerging field is the creation of an unprecedented amount of data. Storage, ownership and expiry of the data become critical issues. It is important to develop artificial intelligence algorithms which could be centralized or distributed based on need.

Visualization: It is critical for an IoT application as this allows the interaction of the user with the environment. With recent advances in touch screen technologies, use of smart tablets and phones has become very intuitive. For a layperson to fully benefit from the IoT revolution, attractive and easy to understand visualization has to be created.

ISSN No. 2395-0900
International Journal of
Engineering Studies and Technical Approach
IJESTA

IV. APPLICATIONS

There are several application domains which will be impacted by the emerging Internet of Things.

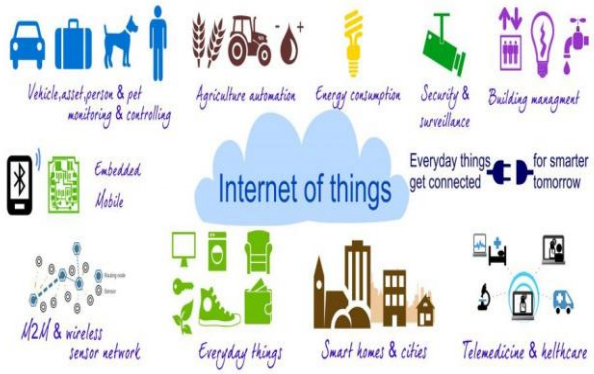

Fig 2. Applications of IoT

The applications can be classified based on the type of network availability, coverage, scale, heterogeneity, user involvement and impact:

Personal and Home: The sensor information collected is used only by the individuals who directly own the network. Usually Wi-Fi is used as the backbone enabling higher bandwidth data (video) transfer as well as higher sampling rates (Sound). Control of home equipment such as air conditioners, refrigerators, washing machines etc., will allow better home and energy management.

Enterprize: We refer to the 'Network of Things' within a work environment as an enterprize based application. Information collected from such networks are used only by the owners and the data may be released selectively. Environmental monitoring is the first common application which is implemented to keep track of the number of occupants and manage the utilities within the building.

Utilities: The information from the networks in this application domain is usually for service optimization rather than consumer consumption. It is already being used by utility companies for resource management in order to optimize cost vs. profit.

V. CLOUD-CENTRIC INTERNET OF THINGS

The vision of IoT can be seen from two perspectives - 'Internet' centric and 'Thing' centric.

The Internet centric architecture will involve internet services being the main focus while data is contributed by the objects.

In the Object centric architecture, the smart objects take the centre stage.

We need IoT application specific framework for rapid creation of applications and their deployment on cloud infrastructures. This is achieved by mapping the proposed framework to Cloud APIs offered by platforms such as Aneka.

ISSN No. 2395-0900
International Journal of Engineering Studies and Technical Approach
IJESTA

Aneka cloud computing platform: Aneka is a .NET-based application development Platform-as-a-Service (PaaS), which can utilize storage and compute resources of both public and private clouds.

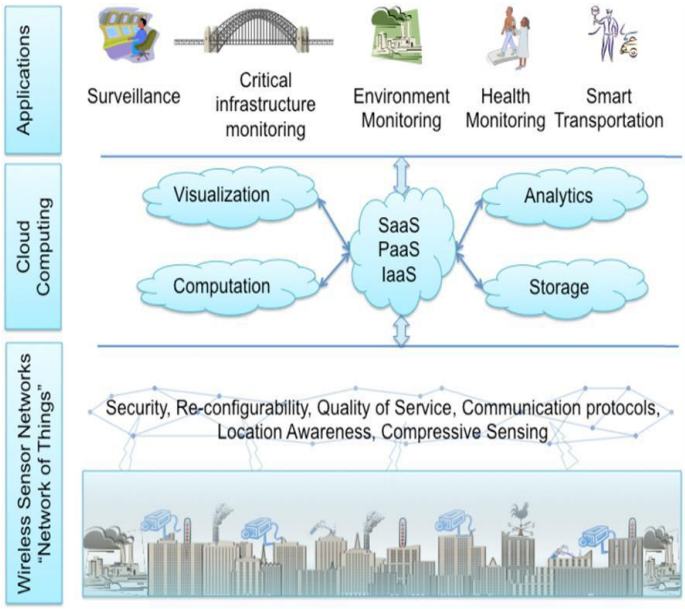

Fig 3. Conceptual IoT framework with Cloud Computing at the centre

VI. ADVANTAGES OF IOT

Some of the most important advantages of IoT are as follows:

Transportation: IoT eases and simplifies the entire process by introducing a monitory sensor that helps to track distance and time locations and other contributing factors.

Inventory Management: IoT is used to tag radio frequency sensors to track the location of products in real time. It has been instrumental in tracking the level of inventory and to stock it in advance, making alerts for unforeseen stoppages, automatically placing orders, etc.

Assessing web user intelligence: IoT is used by third party web data aggregators to have a better understanding of their key customer by tracking them on social media networks to know their preferences.

Integration into Health Care Systems: This could prove to be incredibly beneficial for both an individual and a society. A chip could be implemented into each individual, allowing for hospitals to monitor the vital signs of the patient.

VII. DISADVANTAGES OF IOT

Considering that IoT is still an emerging technology, it has its unfulfilled drawbacks:

Compatibility: Currently, there is no international standard of compatibility for the tagging and monitoring equipment. The manufacturing companies of these equipment need to agree to a standard, such as Bluetooth, USB, etc.

Privacy: In light of the NSA spying revelations, having more information accessible on the web to government agencies, data aggregators, and hackers may not be a comforting thought for members of the public.

Potential of widespread malware: The interconnection of devices could make it much easier for malware to spread throughout a home's integrated system, with results ranging from complete corruption to minor inconveniences.

Complexity: As with all complex systems, there are more opportunities of failure. With the Internet of Things, failures could sky rocket. Infrastructure is still being developed and it will still take quite some time to overcome these disadvantages.

VIII. PRIVACY

Privacy by design. One viable solution is privacy by design, in which users would have the tools they need to manage their own data. The solution is not too far from current reality. Whenever users produce a data fragment, they can already use dynamic consent tools that permit certain services to access as little or as much of that data as desired. Taking that idea a step further, a user in Central Park could provide a location-based service with the information that he's in New York City, but not that he's in a specific park.

Transparency. Transparency is also essential, since users should know which entities are managing their data and how and when those entities are using it. Stakeholders such as service providers must be part of this equation, which might make take-it-or-leave-it license agreements obsolete. Businesses will adjust their services according to the amount of personal data the user provides.

Data management. A huge issue is deciding who manages the secrets. Technically, cryptographic mechanisms and protocols protect data throughout the service's life cycle, but some entities might lack the resources to manage such mechanisms. In other words, one data management policy will not fit all situations. Consequently, there must be policies on how to manage various kinds of data as well as some policy-enforcement mechanism. Developing such data management policies and enforcing them is not trivial. It requires interpreting, translating, and optimally reconciling a series of rules, each of which might be in a different language. And any policies must align with legislation on data protection, which itself could change.

ISSN No. 2395-0900
International Journal of Engineering Studies and Technical Approach
IJESTA

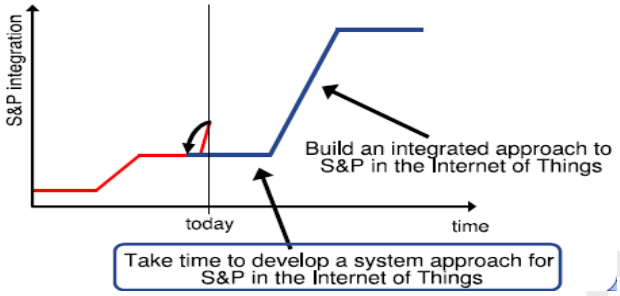

Fig 4.Evolution of S&P with time

IX. SECURITY

While IoT security challenges certainly exist, they are not insurmountable. Stakeholders, vendors and users need to consider and execute the following:

Vendor Management

- The vendors and suppliers of IoT devices need to be tightly controlled to maintain quality and security standards
- Streamline vendors in order to reduce risk of improperly designed or compromised devices

Device Management

- Too many devices to monitor, especially with growing number of cheap sensors
- Better to implement security protocols now and build devices compliant with security protocols than to retrofit devices
- Build in basic permissions management to revoke permissions to a device not authorized to the network any longer

Application Security Measures

- Building security measures into the application itself that leverages IoT will go a long way towards controlling security issues

This includes:

- Secure handshake protocols between communicating devices
- Identity and access management
- Secure connection protocols between all devices
- Storing all identifiable information on servers instead of devices

- Making decisions that allow applications to be user-friendly while remaining secure

The need for increased IoT security measures is widely recognized; however, the path to achieve tighter controls and standardization is far from smooth. The vendor community must collaborate on standardization in order for IoT to help the marketplace.

X. CONCLUSION

In the near future the Internet and wireless technologies will connect different sources of information such as sensors, mobile phones and cars in an ever tighter manner. The number of devices which connect to the Internet is – seemingly exponentially – increasing. These billions of components produce consume and process information in different environments such as logistic applications, factories and airports as well as in the work and everyday lives of people. The society needs new, scalable, compatible and secure solutions for both the management of the ever broader, complexly-networked Internet of Things, and also for the support of various business models.

XI. ACKNOWLEDGEMENT

We hereby thank International Journal of Engineering Studies and Technical Approach (IJESTA) which is a good platform for students to help them grow technically. The open source resources available on the internet have been a boon in helping to find data on the subject in a very fast and efficient manner. Lastly we would like thank our friends who have maintained a tough competition throughout by preparing better paper presentation. Our sincere thanks to those who have motivated us to present this paper.

XII. REFERENCE

i. digitalstrategies.tuck.dartmouth.edu/cds-uploads/people/pdf/SecuringtheInternetof_Things.pdf

ii. nics.uma.es/sites/default/files/papers/1633.pdf

iii. en.wikipedia.org/wiki/Internet_of_Things

iv. www.buyya.com/papers/Internet-of-Things-Vision-Future2013.pdf

v. www.tm.uka.de/doc/gsn09-security-mayer.pdf