Internet of Things: Applications, Security and Research Trends

[1]Neha Kohli
[1] Assistant Professor
[1] Vivekananda Institute Of Professional Studies, Delhi, India

***Abstract*— Internet, the networks of networks makes the world available at the click of the mouse. This paper discusses about Internet of Things (IoT) which is the next evolution of Internet. The objective of IoT is to connect different objects and facilitate their communication. The implementation requires an interaction between different types of hardware and software. Security of information transmitted through such devices is of utmost importance. The areas like data mining, social networking cloud computing, artificial intelligence will extensively be making use of IoT in the near future.**

***IndexTerms*— Internet of Things (IoT), RFID, Wireless Sensor Networks, RFID, Social Internet of Things (SIoT)**

I. INTRODUCTION

The **Internet of Things (IoT)** has been defined as a network of physically connected objects consisting of embedded technology to sense and communicate with the external environment. With the advancement of technology, there are plenty of objects which are being installed with sensors and are having the ability to communicate with one other. The proliferation of these objects in the communication network creates the Internet of Things (IoT) and the embedded sensors help in sharing of information across platforms. The communication in IOT is achieved by providing a unique identity to each and every object. IoT describes a world where devices are connected and communicates in an intelligent fashion than before. "Being connected "not only means use of electronic devices such as smart phones, tablets, laptops, PDA's etc. However in IOT, sensors and actuators embedded within the physical objects are connected through wired and wireless networks and facilitate communication.

The advent of Internet led to networking between people at an unprecedented scale and pace. The next revolution is facilitated by IoT resulting in interconnection between objects to create a smart environment. The fundamental characteristics of IoT are:

Heterogeneity: The devices in IoT are heterogeneous in nature as they are based on different hardware and software.

Interconnection: In IoT anything can be interconnected with the information and communication system.

Dynamicity: The state of IoT devices change dynamically e.g. on/off, connected / disconnected, sleep / waking mode etc.

Scalability: The number of devices that communicate with one another and need to be managed is very large.

II. IOT ARCHITECTURE

IoT connects different devices over the network. This networking environment is heterogeneous in nature. To address this heterogeneity, a 3- layered architecture is proposed consisting of Application Layer, Data Access Layer and the Network layer.

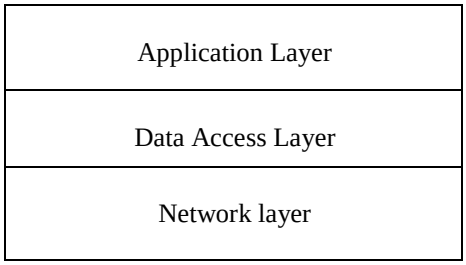

Fig 1 Layered Architecture

Application Layer: In IoT, a large number of devices involved are manufactured by different vendors and they follow different protocols. To facilitate the exchange of information and communication between different devices application layer is required. The role of this layer is to provide a platform where data from different devices can be exchanged.

Data Access layer: In the data access layer, the systems with tags or sensors can automatically sense and exchange information among different connected devices. This layer is integrated with the existing hardware to acquire data.

Network Layer: The networking support is provided by this layer. It allows all devices to be connected together to share information.

III. EASE OF USE ELEMENTS IN AN IOT NETWORK

Corresponding to the three layers in the IoT architecture we can have the following elements in an IoT network:
a) Hardware components comprising of sensors, actuators and embedded communication hardware
b) Data Analysis tools for on demand storage and performing analytics.
c) Presentation tools are accessible on different platforms and are designed for different applications.

In this section, we discuss a few technologies in these categories which will make up the above three elements

1.Radio Frequency Identification (RFID): They help to identify all attached devices automatically [3, 4].Active RFID tags have a transmitter and their own power source which is usually a battery. The power source is used to run the microchip's circuitry. Just as a cell phone transmits signals to a base station, the same way signal is broadcasted to the reader .Passive tags do not possess a battery. Their power source is the reader, which sends out electromagnetic waves that induce a current in the tag's antenna. Semi-passive tags, on the other hand use a battery to run the circuit and communicate by drawing power from the reader. Active and semi-passive tags are useful for tracking high-value goods that need to be scanned over long ranges, such as railway cars on a track, but they cost more than passive tags, which means they can't be used on low-cost items [5, 6].
2. Wireless Sensor Networks (WSN) A wireless sensor network (WSN) consists of a network formed by a large number of sensor nodes .Every node of the network e is equipped with a sensor for detecting physical phenomena such as light, heat, pressure, etc. WSNs are considered as an information gathering mechanism to build the information and communication system which greatly improves the reliability and efficiency of infrastructure systems. Compared RFID technology is used in the embedded communication enabling microchip design for wireless communication of information. With the wired solution, WSNs feature easier deployment and better flexibility of devices. With the rapid technological development of sensors, WSNs will become the key technology for IoT.

3. Addressing mechanism: The ability to identify 'Things' in IoT is important for the success of IoT. Addressing mechanism enables us to uniquely identify trillions of devices and also to control remote devices through the Internet. The most desirable features of creating a unique address are: uniqueness, reliability, persistence and scalability. Each element that is already connected to the network and those that are going to be connected should be identified by their unique identification, location parameters and functionalities.
4. Data storage and analytics: With large amount of data being created there arise a need to analyse this data. Questions like how to store, where to store, till how much time to store become issues to be addressed. Useful information needs t be extracted from this stored data .
5. Visualization: Visualization is essential for an IoT application as this allows the user to interact with the external environment. The front end designed should be easy to understand and very user friendly.

IV. APPLICATION AREAS

A survey done by the IoT-I project in 2010 [1]identified IoTs application scenarios which are grouped in 14 domains viz; Transportation, Smart Home, Smart City, Lifestyle, Retail, Agriculture, Smart Factory, Supply chain, Emergency, Health care, User interaction, Culture and tourism, Environment and Energy.
Real time information about the usage of water can be collected by connecting the meters to a network. This can lead more accuracy in meter reading and reduction in labor cost.
In healthcare, physical activity monitoring can be achieved by smart wearables. The statistics from the smart devices can be sent for remote monitoring.
Energy management can be achieved by introducing smart lighting, cooling and heating systems to save cost and resources.
Smart Refrigerators with a display telling what is inside, food that's about to expire, what all to buy.
Smart parking enables real time monitoring of space availability in the city thereby reducing traffic congestion.
We can see that IoT application space is very diverse and it caters to different set of users.

V. SECURITY AND PRIVACY CONCERNS IN IOT

Connecting things that have been previously unconnected may give rise to unexplored security vulnerabilities. As we interconnect Internet and Other Things, for example, there may be new possibility of hackers, cybercriminals, terrorists, mischief makers and others who wish to do harm

As our devices are becoming smarter day by day, it is necessary to understand what information the devices are collecting and how it is being used or shared. There is an urgent need for implementing security measures that can minimize the impact of a cyber-attack and surveillance of individuals.

The Open Web Application Security Project's (OWASP) List of Top Ten IoT Vulnerabilities sums up most of the concerns and attack vectors surrounding this category of devices:

- Insecure web interface
- Insufficient authentication/authorization
- Insecure network services
- Lack of transport encryption
- Privacy concerns
- Insecure cloud interface
- Insecure mobile interface
- Insufficient security configurability
- Insecure software/firmware
- Poor physical security

An attacker can use vulnerabilities such as weak passwords, insecure password recovery mechanisms, poorly protected credentials, etc. to gain access to a device. Concerns with Web interface include issues such as persistent cross site scripting, poor session management, and weak default credentials. Transport encryption is crucial given that many of the smart devices are collecting and transmitting data that is sensitive in nature. Majority of these devices fail to encrypt network services transmitting data via the Internet and the local network. It is the software which makes these devices functional but no encryption is done during downloading the update files. Privacy should be protected in the device being used, in medium used for storage, during communication process and at processing which helps to disclose the sensitive information [2].

The privacy challenges related to IoT are:

(i) Lack of control and information asymmetry – The communication between devices that communicate automatically, between individuals and other devices, and between devices and back-end systems, which will result in the generation of data flows that are difficult to manage

(ii) Processing of data for intended purpose - Secondary uses of data, inferences from raw information, sensor fusion, make important that at each level IoT stakeholders make sure that the data is used for purposes that are compatible with the original objective of data processing which is known to the user.

(iii) To identify user patterns and profiling - Generating knowledge from abundance of available data will be made easy by the proliferation of sensors which enables very detailed and comprehensive life and behavior patterns

(iv)The limitation on the possibility of remaining anonymous when using services of IoT.

VI RESEARCH TRENDS

The development of IoT infrastructures will identify a few other research trends:

(1) Employing Data mining techniques to create useful information: With so many devices communicating, TB's of data is produced which can be used to extract useful information. All the data needs to be analysed in a timely manner to identify if it is of interest to anyone.

(2) Usage of social networking with IoT: A new paradigm named Social Internet of Things (SIoT) was recently coined by Atzori et al. [8]. SIoT has the capability to support new applications and networking services for the IoT in more efficient ways.

(3) Developing green IoT technologies. Saving energy for future use is a critical design issue for IoT devices such as wireless sensors. The power consumption of powerful sensors is a big concern and limitation for the widespread use of IoT. There is a need to develop energy-efficient mechanisms or approaches that can reduce the power consumed by sensors.

(4) Employing artificial intelligence techniques to create intelligent things or smart objects. Future IoT systems will support features like "auto-configuration, auto-optimization, auto-protection, and auto healing".

(5) Combining IoT and cloud computing. Clouds provide a good way for things to get connected on the go. Cloud of things will have various issues to be addressed like developing models, maintaining networks etc.

VII CONCLUSION

The IoT has become the major disruptive technology bringing a change everywhere. Implementation of security and privacy concerns is of utmost importance in IoT devices. The use of mobile devices, sensors, and remote monitoring equipment is growing at an enormous pace and there will be dramatic advancements in this field. A lot of work needs to be done to facilitate an end-to-end system where devices connect to other networks and the cloud in ways that are interoperable and ensure security. In this comparatively new technology there have been many approaches, concepts, and structures. Various initiatives have already delivered IoT models, architectures, and tools. There is a need for consensus of different approaches, maximize the benefits of IoT while reducing its risks.

References

[1] O. Vermesan, P. Friess,and A. Furness, The Internet of Things 2012, New Horizons, 2012.

[2] Y. Cheng, M. Naslund, G. Selander, and E. Fogelström, "Privacy in Machine-to-Machine Communications: A state-of-the-art survey," International Conference on Communication Systems (ICCS), Proceedings of IEEE, pp. 75-79,2012.

[3] E. Welbourne, L. Battle, G. Cole, K. Gould, K. Rector, S. Raymer, et al., Building the Internet of Things Using RFID The RFID Ecosystem Experience, IEEE Internet Comput. 13 pp 48–55, 2009.
[4] A. Juels, RFID security and privacy: A research survey, IEEE J Sel Area Comm. 24. pp 381–394., 2006.
[5]Klaus Finkenzeller, Fundamentals And Applications In Contactless Smart Cards, Radio Frequency Identification And Near Field Communication, Third edition
[6] Ononiwu G. Chiagozie. Okorafor G. Nwaji, Radio frequency identification (rfid) based attendance system with automatic door unit. Academic Research International Vol.2 No 2 , pp. 168, 2012
[7] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: vision, applications and research challenges," Ad Hoc Networks, vol.10, no.7, pp.1497-1516, 2012
[8] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social Internet of Things (SIoT)-when social networks meet the Internet of Things: concept, architecture