Internet of Things (IoT): A Review on Benefits and Challenges

Nigam Vandana
Assistant Professor
S.S. Jain Subodh P.G. College, Jaipur
svandana94@gmail.com

ABSTRACT - Internet of things is a recent system that affects every aspect of life. It is a Universal Global Neural Network uses cloud technology where variety of devices and objects are connected. IoT is an important technology which comprised of smart devices and machine communicating each other. Communication among devices, objects and machines produces voluminous data that must be stored and processed properly and is capable to command and control the things to make life easier. IoTserves as a basis for smartcities, smart buildings, smart healthcare and other applications. This review paper puts light on IoT applications and challenges that facing the implementation of IoT.

KEYWORDS – Internet of things, Internet, Network, Security, Smart Devices

1. INTRODUCTION

Internet of Things, or IoT is basically a system where computing devices, objects, human beings, digital or mechanical machines having unique identifiers (UIDs) are interconnected with each other and are able to transfer data with any human or computer intervention. Multiple technologies like Real Time Analytics, Machine Learning, Embedded System, Control System, Automation and Wireless Sensor Network are involved in IoT [1]. The term IoT was first coined **Kevin Ashton** in a presentation to Proctor & Gamble in 1999, but now the definition is more inclusive and covers wide range of applications.

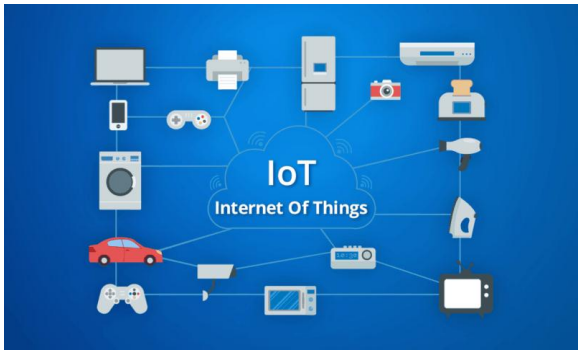

Fig 1: IoT

In a nutshell, IoTprovides a concept to connectdiversified devices to the internet and permits them to communicate with each other over the internet as shown in figure 1. IoT is a massive network of connected deviceswhich collect and allocate data about how they are used and the environments in which they are operated [2]. Here devices basically learn from other devices by experience just like human beings. Basic concept of IoTis interact, contribute andcollaborate to things.A room temperature sensor is capable to collect data and sends it across the network, here various device sensors are used to so that temperatures can be adjusted accordingly.

This paper comprised of four sections. Section I describes the background and related work, section II puts light on Benefits of IoT and Domains of IoT and section III puts light on major security issues.

2. BACKGROUND

IoT is a recent research area attracting attention of researchers. Today it is in its developing stage and soon it will grab the entire world and there will probably no area remain left that in not using IoT. This section discusses the work done in IoT reference. Authors in their paper [3] in their review paper discuss current research, key enabling techniques, IoT applications, research trends and challenges in concern area. Authors [4] present a framework for realizing energy efficient smart homes based on wireless sensor networks and human activity detection. When users are at home, most of their activities related to set of electrical home appliances which used energy to perform their task. Here basic need is to monitor the energy consumption by the appliance so that real consumption of energy and wastage of energy can be detected correctly and to reduce the wastage.

Authors in survey paper [5] discuss the existing works on tenancy monitoring and multi-modal data fusion techniques for smart commercial buildings. The aim is to lay down a frameworkfor future research to use the spatio-temporal data obtained from one or more of various IoT devices such as surveillance cameras, RFID tags, temperature sensors that may be already in use in the buildings.

This paper [6] mainly focuses on an urban IoT system which focuses on survey of enabling technologies, style and protocols.are designed to support the Smart City vision. This aims at exploiting

the most advanced communication technologies to support added-value services for the administration of the city and for the citizens.

3. BENEFITS OF IoT

IoT is gaining popularity because it is not only revolutionizing the daily life but helps to make its users better and comfortable [7]. In recent years a broad range of devices are included in daily life of users. Such devices includes a variety like medical, household appliances, traffic control, digital assistants like Google home, Amazon Alexa, I-phone Siri etc.

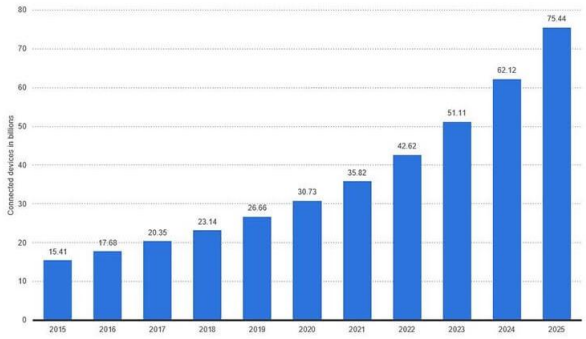

Fig 2: IoT connected devices installed base worldwide from 2015 to 2025 (in billions)(Source Statista)

According to the Gartner report, by 2020 connected devices across all technologies will reach more than 20.6 billion. As per the Cisco report, IoT will generate $14.4 trillion in value across all industries in the next decade. The increasing exploitation of various devices has enabled new use cases for network technologies. Some experts predict that the IoT may generate as much as US$13 trillion in revenue by 2025.The above figure shows that in year 2020 the connected devices worldwide will be 30.73 billion and will reach to 75.44 billion in 2025 which is more than three times. It not only generates the number of devices at a fiery rate but the data produced by them would also be increased proportionally. IoT is going to grab a wide marker place in near future [8].

Since IoTtechnique enables users to remotely access and control devicesacross the internet and provides opportunities to directly connect & integrate the physical world to the computer-based systems using sensors and internet. The interconnection of these multiple embedded devices will be resulting in automation in nearly all fields and also enabling advanced applications. The visible benefit of IoT is improved accuracy, efficiency and economic benefit with reduced human intervention. It encompasses technologies such as smart grids, smart homes, intelligent transportation and smart cities. The major benefits of IoT are:

- **Technical Optimization** – With IoT it is possible to improve technologies and make them much better for users. Sensors generate data and the same data is collected by manufacturer so that data can be analyzed, elaborated and used to make better design and make them efficient and useful.
- **Reduced Waste** –IoT provides real-time information which leads to effective decision making & management of resources. For instance if there are multiple faults in the engines, the manufacturer can track the plant and can resolve the defects related to manufacturing units.
- **Improved Customer Engagement**-Automated actions can improve the customer experience. For example if there are some issues related to a car is detected by sensors, then such issues are noticed at same time by manufacturer also so that the faulty parts can be made available at service station at the same time.

4. IOT ACROSS VARIOUS DOMAINS

a) Government

IoT can be used as a basic technique for government to built smart cities. It can also be used to provide better security across border through high performance and smart devices. It also helps government agencies to observe data in real-time and get better services like healthcare, transportation, education etc.

Healthcare Application

Healthcare applications are also revolutionized by IoT. It provides opportunities to users to monitor their health activities using smart gadgets like smart watches, fitness devices etc at regular intervals. Data gathered by multiple healthcare applications can be used to analyze different diseases and find their better solutions.

b) Education

Various education aids are developed and used with the help of IoT to fulfill gap in education sector. Improvement in performance and response of students, optimization of cost, improvement in management can be achieved using IoT that could be helped in achieving the quality education to a high level.

c) Air and Water Pollution

Various sensors and devices can be used to detect water and air pollution which ultimately helps in preventing the disasters and contamination. With IoT it is possible to detect changes in crops, climate and soil changes and helps in reducing the related

problems. Human intervention can be reduced in farming analysis and monitoring with the help of IoT.

d) Transportation

Transportation sector is also revolutionized by IoT. Driverless cars, automatic controlled traffic lights, parking assistance are some prominent examples of IoT technology that has changed the traditional transportation to modern one. Current states of the vehicles are also sensed by sensors and drivers don't face any issues while travelling.

e) Marketing of Product

Marketing of products is a prime need for its sales promotion and IoT is a smart and intelligent method to encourage marketing of products and respond to customer fondness by delivering pertinent content and solutions which helps in improving business strategies in real time scenario.

With the advancement in technology, numerous devices are using sensors, actuators, embedded computing and cloud computing. Communication between devices makes it possible to share information without human intervention and can be exploits in various domains of life.

5. SECURITY ISSUES OF IOT

IoT has revolutionized the lifestyle and provide many facilities to users but raising popularity has raised many serious security issues also. Identity theft, Cyber attack, password attacks, security vulnerabilities are very serious issues associated with internet and IoT. Cyber criminals can get remote access to devices and cause chaos on the devices or users.

Major Security issues are discussed here

a) Secure Constrained Devices

Generally IoT devices have limited memory, processing capability, storage and operate on lower power and these constrained devices can only employ fast and lightweight encryption hence they are not fit for heavy and complex encryption-decryption quickly to transmit data securely in real time environment. Apart from this, such devices are often susceptible to side channel attacks also. To apply proper security to such devices it is necessary to use multiple layer of security, firewall etc. so that security can be enhanced.

b) Authorize and Authenticate Devices

Device authorization is a method through which device can establish their identity before they access gateways and upstream apps and services. If device authentication may fail due to weak password authentication, password unchanged from their evade values or some other reason further communication may be stopped. So for uninterrupted services authorization and authentication of devices is an essential step for using IoT.

their default values.

c) Secure Communication

A very big challenge to secure devices is to ensure that there must be secure communication across the network among devices, apps and cloud services. If messages are not encrypted before sending them over the network, there would be a chance for hackers to steal or modify the confidential data. It is very necessary to isolate devices using secure and private communication so that data can be transmitted in confidential manner, so that data transmitted remains confidential.

d) Ensure Data Privacy and Integrity

When data is transmitted across network, it must be processed and stored very securely. Implementing data privacy includes redacting sensitive data before it is stored or using data separation to decouple personally identifiable information from IoT data payloads.Data that is not of use and will not be required must be disposed very securely to avoid any discrepancy; stored data should be managed with legal and regulatory framework for its future use. Use of digital signature, checksum is some popular methods that can be implemented on data to maintain its integrity [9].

e) Secure Web, Mobile and Cloud Applications

To manage, process and access IoT devices and data, world wide web, mobile and cloud applications are used very popularly. To make this transaction very secure it is necessary that multi-layered approach to IoT security should be implemented to enhance security.

f) IoT Malware and Ransomware

IoT is a preferred choice for smart technologies hence number of connected devices is also increased proportionally. Unfortunately number of ransomware and malware also increases to deed them. Attack on device and data ultimately limit or disable device functionality and steals data at the same time. It is very necessary to protect the system from such attacks and keep them secure against such vulnerabilities.

g) Untrustworthy Communication

Encryption is a basic need to send message to network securely. If messages are send without

encryption there is strong possibility that it's security can be compromised and message can be theft, altered, modified and deleted. The biggest IoT security challenge is to apply high level encryption so that cloud services and devices can be kept secure.

h) AI and Automation

IoT is now a part of daily life. Due increased number of users and data generated by them is so voluminous that traditional data collection and networking methods and data handling methods are not sufficient to handle this big data. Artificial Intelligence tools and automation are some preferable choice to manage such giant data. Data specific rules are designed and traffic patterns are identified to manage them efficiently.

i) Detect Vulnerabilities and Incidents

In large IoT systems as the number of attached devices, apps,communication, services protocols etc. are involved and grow proportionally then it becomes very difficult to know that at what time some incident has occurred. Hence an essential step is to make proper strategies to prevent vulnerabilities, breaches, log anomalies etc. Various methods like ethical hacking to detect vulnerabilities, penetration testing, security intelligence etc. are designed and implemented on system to stop such activities and keep system secure from problems [10].

j) Predict and Preempt Security Issues

A longer-term IoT security challenge is to apply security intelligence not only for detecting and mitigating issues as they occur, but also to expect and proactively protect against potential security threats. Other approaches include applying monitoring and analytics tools to correlate events and visualize unfolding threats in real-time, as well as applying AI to adaptively adjust security strategies applied based on the effectiveness of previous actions.

6. CONCLUSION

It is clear that Internet of Things (IoT) is a revolutionizing technology, changing the way of living style and it is the future for coming decade. The propagation of devices with improved communication capabilities makes it possible to connect and use them in an efficient way. It is an ideal emerging technology to affect and influence various domains. Security is an important concern in IoT that gains attention of researchers. In this paper we have discussed various challenges faced that can be a research opportunity in security of it.

7. REFERENCES

[1]https://en.wikipedia.org/wiki/Internet_of_things

[2]https://www.cigionline.org/articles/emerging-internet-things?gclid=EAIaIQobChMI5e-62sab5AIVm IRwCh0X- QMHEAAYASAAEgLFS_D_BwE

[3] Li Da Xu, Wu He, and ShancangLi,"Internet of Things in Industries: A Survey" IEEE transactions on industrial informatics, vol. 10, no. 4, November 2014.

[4] laaAlhamoud, Felix Ruettiger, Andreas Reinhardt, Frank Englert, Daniel Burgstahler, Doreen Bohnstedt, Christian Gottron and Ralf Steinmetz," SMARTENERGY.KOM: An Intelligent System for Energy Saving in Smart Home", 3rd IEEE international workshop on global trends 2014

[5] Kemal Akkaya, Ismail Guvenc, RamazanAygun , Nezih Pala, Abdullah Kadri," IOT-based Occupancy Monitoring Techniques for Energy-Efficient Smart Buildings" ,2015 IEEE wireless communication and networking conference.

[6] Andrea Zanella, Nicola Bui, Angelo Castellani,LorenzoVangelista, and Michele Zorzi, "Internet of Things for Smart Cities" IEEE Internet of things journal , Vol. 1 , No. 1 , FEBRUARY2014.

[7] https://www.edureka.co/blog/iot-tutorial/

[8] https://internetofthingswiki.com/iot-security-issues-challenges-and-solutions/937/

[9] https://www.peerbits.com/blog/biggest-iot-security-challenges.html

[10] Zeinab, K. A. M., &Elmustafa, S. A. A. (2017). Internet of Things applications, challenges and related future technologies. World Scientific News, 2(67), 126-148.

[11] Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017).A survey on security and privacy issues in Internet-of-Things. IEEE Internet of Things Journal, 4(5), 1250-1258.

[12] Stankovic, J. A. (2014). Research directions for the internet of things. IEEE Internet of Things Journal, 1(1), 3-9.

[13] Gubbi, J., Buyya, R., Marusic, S., &Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660.

[14] Vashi, S., Ram, J., Modi, J., Verma, S., &Prakash, C. (2017, February). Internet of Things (IoT): A vision, architectural elements, and security issues. In 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 492-496). IEEE.