Visvesvaraya Technological University, Belagavi –590018

TECHNICAL SEMINAR REPORT ON

"IoT:Challenges and Issues in Indin Presoective "

Submitted in partial fulfillment of the requirements for the award of

BACHELOR OF ENGINEERING IN
ELECTRONICS AND COMMUNICATION ENGINEERING

For the Academic year 2021-2022

Submitted By

ATHUN LAL P

4SH18EC003

Under the Guidance of

Mrs. Chitra Prabhu M
Asst. Prof., Department of ECE

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

SHREE DEVI INSTITUTE OF TECHNOLOGY, MANGALURU- 574 142

SHREE DEVI INSTITUTE OF TECHNOLOGY

(An Institution under VTU, Belagavi)

MANGALURU- 574 142

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

CERTIFICATE

This is to Certified that the Technical Seminar entitled **"IoT: CHALLENGS & ISSUES IN INDIAN PERSPECTIVE"** is a bonafide work carried out by **ATHUN LAL P** bearing USN **4SH18EC003** respectively in partial fulfillment for the award of degree of **Bachelor of Engineering** in **Electronics and Communication Engineering** of the Visvesvaraya Technological University, Belgavi during the year 2021-2022. It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the report deposited in the departmental library. The Technical seminar report has been approved as it satisfies the academic requirements in respect of Technical seminar work prescribed for the degree of Bachelor of Engineering.

_____ _____

Signature of the Guide Signature of the HOD

Mrs. Chitra Prabhu M **Mrs. Chitra Prabhu M**

B.E, MTech **B.E, MTech**

ABSTRACT

Internet of Things is the Connections of embedded technologies that contained physical objects and is used to communicate and intellect or interact with the inner states or the external surroundings .Rather than people to people communication, IoT emphasis on machine to machine communication.

This paper familiarises the status of IOT growth In India, and also contains security issues challenges. Finally, this paper reviews the Risk factor, security issues and challenges in Indian perspective.

ACKNOWLEDGEMENT

The satisfaction and euphoria that accompany the successful of any task would be incomplete without the mention of the people who made it possible, whose constant guidance and encouragement crowned my efforts with success.

I would like to profoundly thank my ELECTRONICS & COMMUNICATION department for providing such a healthy environment for successful completion of a Technical Seminar Report. I would like to convey my heartfelt thanks to **Management** for providing me with the good infrastructure, laboratory, and facility, qualified and inspiring staff whose guidance was a great support to me in our seminar completion.

I would like to thank **Dr. K.E Prakash, Director and Principal, SDIT, Mangaluru** for his continuous support.

I thank **Mrs. Chitra Prabhu M, Head of Department of ECE, SDIT, Mangaluru** for her valuable guidance and support.

I would also like to thank all my staffs of Electronics & Communication department who have been directly or indirectly helped me in the completion of a Technical Seminar report.

And lastly I would hereby acknowledge and thank my parents who have been a source of inspiration and also instrumental in the successful completion of a Technical Seminar Report.

DECLARATION

I, **ATHUN LAL P** bearing USN **4SH18EC003**, student of VIII Semester BE in Electronics and Communication Engineering, Shree Devi Institute of Technology hereby declare that the Seminar entitled **"IoT: Challenges & Issues in Indian Persepctive"** has been carried out and submitted in partial fulfilment of the requirements for the degree of **Bachelor of Engineering in Electronics and communication Engineering** of Visvesvaraya Technological University, Belagavi during the academic year 2021-2022.

Date: **Athun Lal P**

Place: **4SH18EC003**

CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

In the succeeding coming years, it will have major effects on business models, infrastructure,security and trade standards, during the complete IT computing and networking systems. TheInternet of Things is a new light of technology progression in the early stages of market growth. IOT has the potential to speed up the "sharing economy." So as offering new techniques to manage and track minor things, it will also allow the sharing of new, minor andeconomical items outside the communities, aircrafts, cars and motorbikes.

As it trends go on, it will offer exclusively novel applications, that will drive new business prototypes and profit prospects .It pushes devices and sensors to more granular levels and enables the creation of new uses, new applications, new services and new business models that were not previously economically feasible. It will also dangerous for lots of current industries.

Today, in worldwide IoT Technology is among top 5 technologies according to Gartner's Chart. That means, It is highly used in different sector in different role either it is in smart homes or vehicle tracking, kids and old age peoples monitoring or daily routine job. However at present the actuality is that these segments hire several IoT enabling devices, and future is already fragmenting of the new revolution.

CHAPTER 2

Architecture of IoT and Challenges

Internet of things (IoT) architecture is an ecosystem of connected physical objects that are accessible through the internet. The 'thing' in IoT could be a person with a heart monitor or an automobile with built-in-sensors (i.e., objects that have been assigned an IP address and have the ability to collect and transfer data over a network without manual assistance or intervention).

The embedded technology in the objects helps them to interact with internal states or the external environment, which in turn affects the decisions taken. IoT world where all the devices and appliances are connected to a network and are used collaboratively to achieve complex tasks that require a high degree of intelligence, and IoT is an interaction between the physical and digital words using sensors and actuators.

Furthermore, the IoT architecture may combine features and technologies suggested by various methodologies. IoT architecture is designed where the digital and real worlds are integrating and interacting constantly, and various technologies are merged together to form IoT.

There are different phases in the architecture of IoT but they can vary according to the situations but generally, there are these four phases in the architecture of IoT.Internet of Things (IoT) is a system of interrelated, internet-connected objects which are able to collect and transfer data over a wireless network without human intervention.For example, smart fitness bands or watches, driverless cars or drones, smart homes that can be unlocked through smartphones and smart cars, etc.

CHAPTER 3

Issues in Information Systems

Internet of Things (IoT) has become one of the cutting-edge technologies and an attractive area of interest for the research world, and economically attractive for the business world. It involves the interconnection of multiple devices and connections of devices to humans. IoT requires a cloud computing environment to handle its data exchange and processing. At the same time, it requires artificial intelligence (AI) to analyze the data stored at cloud infrastructure and make fast and reliable intelligent decisions.

These interconnected IoT devices use their unique-identifiers and the embedded sensor with each device to communicate with each other, and exchange information among them using an Internet and cloud-based network infrastructure (Girma, 2018). We are living in the era of big data where the necessity of applying AI/ML has been very critical to the process and analyze the collected cloud-based big data fast and accurately. However, even though AI is currently playing a vital role in improving the traditional cybersecurity, both the cloud vulnerability and the networking of IoT devices are still major threats.

Besides the security issues of cloud computing, IoT devices, and AI is being used by hackers and continues to be a threat to the world of cybersecurity. Moreover, most of wirelessly accessed IoT devices deployed on a public network are also under constant cyber threats. This research paper will propose a hybrid detection model as a solution approach using artificial intelligence and machine learning (AI/ML) to combat and mitigate IoT cyber threats on cloud computing environments both at the host-based and network level. KEYWORDSIoT security; cyber threats, Cloud Computing, artificial intelligence, machine learning.

Published 4 times a year, Issues in Information Systems (IIS) journal is a refereed (double-blind peer review) publication (ISSN 1529-7314). IIS publishes the latest research in practice and pedagogical topics that focus on how information systems are used to support organizations or enhance the educational process.

CHAPTER 4

Big Data & Disruptive Computing Platforms Braced Internet of Things: Facets & Trends

The Internet of Things (IoT) has been evolving in tandem with centralized cloud computing to fog computing, edge computing, Semantic computing, etc. Pervasive IoT applications like Healthcare applications generate a huge amount of sensor data and imaging data that needs to be handled rightly for further processing. In traditional IoT ecosystem, Cloud computing ensures solution for efficient management of huge data with its ability to access shared resources and provide common infrastructure in a ubiquitous manner.

Majority of the IoT applications are highly sensitive to time and necessities latency bounded execution. There is time delay introduced when the data transmission occurs between the cloud and the application which is unacceptable. This chapter will disclose the various facets and trends in the integration/coupling of evolving computing platforms and disruptive technologies like Fog/Edge Computing, Big Data, blockchain with IoT that overcomes challenges existing in the traditional deployment of IoT environment. Further, there are several issues with IoT and Cloud Computing framework like each individual part of the IoT architecture could act as a point of failure that can interrupt the whole network and secondly, the centralized cloud model is vulnerable to loss of integrity of data. This chapter will review and reveal the trends in bracing computing approaches, managing the huge data using datacenters in Internet of Things ecosystem.

The review is advocated with a case study on waste management system applied with the fog/edge computing and cloud computing. Further, various trends in applicability of block chain in the IoT ecosystem is also reviewed. This chapter discusses the fundamental facets of various computing paradigms and approaches that may help to address issues of big data through creating IoT ecosystems.

CHAPTER 5

Role of IOT in India

Government initiatives, supporting environment, good living standards and increasing approval of smart applications plays the vital roles in the growth of market.

According to the report of COMSNETS in 2015 [1], Government think about to invest in IOTfor developing approximate 100 Smart cities its approximate proposed cost is ₹7060 crores Although according to Indians requirement, IOT product are useful in each domain and variouscompanies invest in lots of sector and this percentage is increase day by day, but focus on SmartWater Management, Smart Environment, Healthcare, Smart Agriculture, Smart Waste Management, Smart Safety, Smart Supply Chain, etc.

But according to the Indian economy factor affordability to a billion population is very difficult. Supporting environment and Indian Infrastructure like power supply, poor pollution,extreme temperatures, high levels of humidity and dust, No clean and poor telecom coverage.

Fig.5.1 Future of IoT

The highest rated priority project by Indian Government is **Digital India Program** which is used for encouragement of digitalisation, and make India as a digital empowered country and knowledge economy, is expected to provide therequired motivation for expansion of the IoT productiveness ecosystem in the country.
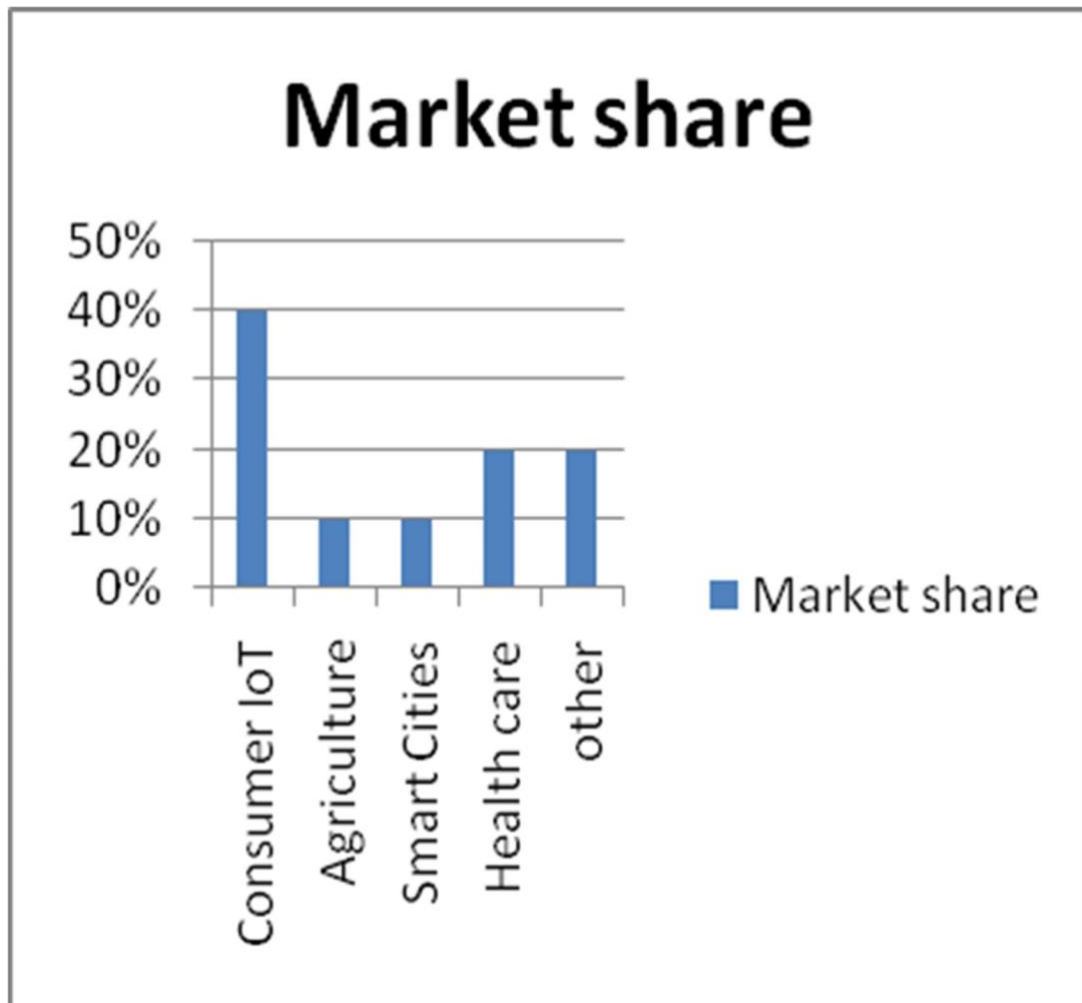

Fig.5.2 Market Share

CHAPTER 6

Challenges of the Internet of Things

6.1 SECURITY

Security is an essential pillar of the Internet while the major challenge for the IoT. As the time goes the trend of IOT inflates from millions of devices to tens of billions. As increasing the number of connected device the chance to exploit safety vulnerabilities is also increase, like in cheap or low standard designed devices, due to incomplete data streams the chances of data theft is increased by which people's health and safety can be risky.

The highest rated priority project by Indian Government is Digital India Program which is used for encouragement of digitalisation, and make India as a digital empowered country andknowledge economy, is expected to provide the required motivation for expansion of the IOTproductiveness ecosystem in the country.

Many IoT arrangements will also include collections of similar or adjacent similar devices. This homogeneity expands the potential impact of any single security weakness by the total number of devices that all have the same features.

6.2 PRIVACY

As Authenticity, trustworthiness and Confidentiality are important aspects there are some other requirements also important like discriminatory access to certain facilities, preclude them from shared with other things at certain Times and business communications involving smart objects would need to be secure from opponents. The data networks are still delicate and also costly in comparison of other developed country.

From an Indian perspective, the cloud storage operation is still in the merging stage Transmit the data to a cloud service for processing, sometimes includes a third party. The gathering of this information leaks legal and regulatory challenges facing data protection and privacy law.

In order to realize the opportunities of the IOT, Some new strategies will be required for privacy choices through a broad range of expectations, while still development innovation in new technologies and services.

6.3 STANDARDS

Absence of standards and documents can assist Senseless activities by IOT devices. Low standard or cheap designed and configured devices have undesirable consequences for the networking resources. Without standards to guide developers and manufacturer sometimes design products that operate in disruptive ways on the Internet. When any technology have standard development process then it can be easily available everywhere and can used by all applicants, and increase the growth also. While in today's world, global standards are followed by every local station.

6.4 TRAINED WORKFORCE

Implementation of every technology requires team of skilled persons those have ample knowledge of network, hardware, software and about that technology. And India is backward in this point where manpower think when technology is spread they lose their job and there is no life of new technology. So they don't take any initiative to lean about it. So every organisation face lots of problem during their changeover phase from the legacy systems to IoT enabled systems.

Fig 6.1 Scope of IoT

CHAPTER 7

REVIEW OF SURVEY

S.N	Survey	Citation	Year	Security & Risk Factor	Challenges
1.	The Internet of Things for Health Care: A Comprehensive Survey.	[4]	June, 2015	-Computational Limitations -Memory Limitations -Energy Limitations -Scalability -Mobility -Communications Media -Data Protection	-Standardization -IoT Healthcare Platforms -Cost Analysis -Technology Transition -The Low-Power Protocol -Scalability
2.	A Survey on Challenges, Technologies and Applications of IoT.	[5]	March,2016	-Front end sensors and equipment –Networks -Backend of its System	-Scalability -Device Heterogeneity -Energy Optimized Solution -Ubiquitous Data Exchange Through Wireless Technology -Self-Organization Capabilities -Semantic Interoperability and Data Management
3.	Internet of Things (IoT) : Challenges and Future Directions.	[6]	March,2016	-As IoT connects more devices together it provides more decentralized entry points for malware -Trust and Privacy.	-Standards and interoperability -Complexity, confusion and integration issues. – Internet connectivity and power requirement.
4.	Smart Home Analysis in India: An IOT Perspective.	[7]	June,2016	-Unique identification low security at the server side. -Privacy - Authentication	-Reliability -Co-ordination among connected objects, -Integration of several devices increases the system complexity and connectivity problems.

5.	Challenges and Risk to Implement IOT in Smart Homes: An Indian Perspective	[8]	Nov, 2016	-Risk is to store the sensitive data either on local server or to use VPN in case using the remote server of vendor. -When Security system based on the CCS (Centralized Controlled System) for processing, application and data storage, then a risk of central point of failure is increase. -End point protection, Trust & Safety, Physical Security. -Hacking, DoS , updation, virus , password based attacks and phishing	-Internet connectivity, consistency and accessibility of necessarysignals bandwidth. -Cost of technology. -Poor supporting organizational setup. -IoT adoption due to nonexistence of welltrained staff. -Lack of awareness of IoT Systems, Services and Applications.
6.	Health Care Systems Using Internet of Things.	[9]	December, 2016	Data security causes concerns in the implementation ofIoT in healthcare.	-Lack of HER system integration. - Interoperability challenges keep IoT data in different silos. -IoT data alone may not be as meaningful if it is not within the context of afull health record. -Constant changes in hardware and connectivity technology.

CHAPTER 8

CONCLUSION

Finally, the future of IOT becomes a worth but massive amounts of data increased its complexity in detection, communications, controller, and in producing awareness but its growth will be increased day by day .Although future of IOT will be predictable to be integrated, all-in-one, and ubiquitous. Service organization required to be enclosed in a set of standards. So, As an Intelligent.

System progresses of IOT can be decided with the cooperation of interoperability, awareness, skilled, teamwork, energy sustainability privacy, trust, confidentiality, and security. IOT has become an expected trend of development of information industry. This will outcome in quality of lifestyles. This paper surveyed some of the most important issues and challenges of IOT in Indian perspective like what is being done and what are the issues that require further improvement.

Some possible improvements include adding a facility to handle unified, seamless, and universal internet connectivity, standardization, within interoperability. Energy sustainability privacy, and security are also major point on which research can go on.
In the coming years, improving these challenges will be a powerful and bold step for networking and communication in commercial, industrial and academic area.

REFERENCES

[1] IoT –" Challenges and Opportunities in Indian Market", COMSNET, Bangalore IndiaJanuary.

[2] SurendraDhote, "Internet of Things (IoT) Market in India",April 24, 2017.

[3] "2nd Internet of Things India expo 2018", Delhi.

[4] M.Suruthi ,D.Nivetha "A Survey on Challenges, Technologies and Applications of IoT", IJARCCE ,Vol. 5, Issue 3, March 2016.

[5] Ms.YogitaPundir ,Ms. Nancy Sharma , Dr. Yaduvir Singh, "Internet of Things (IoT) : Challenges and Future Directions ",IJARCCE, ISSN 2278-1021 Vol. 5, Issue 3, March 2016.

[6] ChinmayaVyas,ShashikantPatil, "Smart Home Analysis in India:An IOT Perspective" ,Mumbai,IJCA (0975 – 8887) Volume 144 – No.6, June 2016, 29 .

[7] RakeshRoshan ,Abhay Kr. Ray , "Challenges and Risk to Implement IOT in Smart Homes: An Indian Perspective", IJCA(0975 – 8887) Volume 153 – No3, November 2016,16.

[8] AkshayGapchup, AnkitWani, DurveshGapchup, and ShashankJadhav, "Health Care Systems Using Internet of Things ",IJIRCCE Pune, India,Vol.-4,Issue-12,December2016.