Challenges in Internet of Things

Venkataraman Balaji, P. Venkumar, Sabitha M. S., Vijayalakshmi S.

Abstract—Internet of Things (IoT) or Cyber Physical systems (CPS)denote culmination of inter connected equipment, sub systems, objects and living things with notable identifiers (UIDs) and has the capability to exchange information in the network without human or machine intervention. The real benefit of IoT is to establish a smart communications with the current systems and make the information visible to everyone. This paper discusses various challenges in IoT related to security, data management, identity management and network related issues

Keywords—IoT, Cyber Physical systems, Security

I. INTRODUCTION

The Internet of Things is the latest wave of revolution in information technology that exponentially enables comprehensive interoperability of systems and thereby resulting in intelligent and timely decisions [1]. It was introduced by Electronic product code (EPC) Technology and research work of International Telecommunication Union (ITU) .From the days of enabling just human connectivity through emails and social networking, now evolved the possible connectivity of objects and people for instant monitoring and sophisticated actions. This also means that location is no more a barrier, remote accessibility helps to accomplish seamless interconnection. Internet is the conduit by which any ‘Thing’, may it be a device or living thing could be connected enabling both information sharing (passive) and if desired automated actions (actuations).

The benefits of IoT are easy communication, automation and control, intelligent information, efficient monitoring, lesser time consumption, reduced man power, better quality of life. As much as it is benefitting, it has its own challenges like poor compatibility, more complexity, lessprivacy, higher energy consumption, immense initial cost, unprecedented security and safety. While IoT is a big revolution by all means, it also understandably has several constraints.

This paper covers the issues that are faced by IoT. The main challenges are possible breach of privacy, reliability, ownership of data among the keystone players, confidentiality of data and related security. In the modern technological age numerous threats are encountered by the users due to insecure IoT systems. If a vehicle is tagged with RFID, this also means a privacy threat to the occupants of the vehicle [1]. If not secured thoroughly, hackers could play the spoilsport by manning the healthcare data and intentionally alter Doctor’s diagnosis, resulting in fatal consequences [1]. Similarly in Warfronts, enemies could intrude the wireless sensors to generate false information resulting dire and irreversible losses. An untrusted IoT server can misuse user’s data and information. High-tech modern cars that use insecure IOT Technology can be easily controlled by an intruder. An individual’s privacy should not be compromised with advent of technology however good it is. The Legal framework and underlying policies needs to be strengthened for protection against wrong usage of IoT technology, thereby winning better acceptance by common mankind.

The views and recommendations of various researchers related to IoT challenges are discussed in section 2.

II. LITERATURE REVIEW

The updated IoT technology related papers are gathered, collectively reviewed and illustrated below.

Charu C. Aggarwal et al. [2] discussed about various challenges related to sensor data collection and data processing. Various big data analytical tools and processing methodologies were elucidated. Scalability challenges, computational overheads involved in processing, IP addressability , privacy , security, data management and related issues were addressed in the paper.

JayavardhanaGubbi et al. [3] covered detailed information about current vision and intent of Internet of Things (IoT), with a fresh approach in definingvarious possible domains of application, how IoT could be realised around cloud and possible future trends in Cloud Centric Internet of Things. The scientific challenges in order to handle huge potential of wireless sensor modes were discussed. The importance of cloud based storage, cloud based analytics and visualisation, video based IoT were provided. Also it discussed about architecture, security protocols, energy efficiency and service quality.

Ala Al-Fuqaha et al. [4] gives an overview of IoT, its protocols and its applications. The latest development in internet technology, mobile application and machine to machine communication are the building blocks of IoT. In future IoT will build a bridge in numerous technologies to bring out new applications by connecting physical objects for intelligent decision making. In order to handle huge amount of objects, appropriate protocols were suggested to avoid network congestion. NIU Ling et al. [1] explained the remote data monitoring system, characteristics of data processing and visualisation techniques using IoT.

Revised Manuscript Received on December 29, 2019.

* Correspondence Author

Venkataraman Balaji *, President, TVS Sensing solutions private limited, Madurai, Research scholar, Kalasalingam academy of research and education, Krishnan Koil. Email: balaji.v@tvsss.co.in

Dr.P.Venkumar, Senior Professor, Department of Mechanical Engineering, Kalasalingam academy of research and education, Krishnan Koil. Email: p.venkumar@klu.ac.in

Dr.Sabitha.M.S, Head Informatiion Systems, TVS Sensing solutions private limited, Madurai. Email: sabimurali@rediffmail.com

Dr.S.Vijayalakshmi, Associate professor, Thiagarajar college of Engineering . Email: svlcse@tce.edu

Other than RFID technology ,new technology suggest near field communication, QR code, bar code and digital water marking can be used for linking various things . Introduction of arduino will assists with a connectivity for computer or laptop to realise IoT over internet. M.Suresh, et al.[5] expressed about the various security measures that can be taken to improve IoT system's stability and safety. Various challenges faced by the IoT and its solution are discussed in this paper. This paper proposed an IoT based airport parking system implemented using arduino environment.

Qihui Wu et al. [6] a discussion about the cognitive based IoT is done. It explains about the objects having the capability to learn ,think , and execute results by themselves. CIoT proposed a new knowledge based learning methodology to improve the converging speed and attain greater performance. The keen objective of the paper was to bring the theory into practice. Rodrigo Roman et al. [7],extensively discusses about how to secure the internet of things. TobiasHeer et al. [8] discusses about the challenges faced by IP based internet of things system.

Section 3 explains the common IoT challenges and related mitigations .

III. CHALLENGES AND MITIGATION TO IoT

Creating a secured IoT network requires strenuous efforts due to the various technologies available to interconnect the components of the IoT network and its highly distributed nature. Additionally the trade off made between ease of service or access of maintenance and the protection against the unintentional physical damage in locating the network also pose challenges. Other environmental elements present also pose challenge to the security of IoT network.

To overcome these challenges the IoT must have be build considering end to end security needs of all IoT network elements from the identification of network components to providing reliable service, from data capturing method to the ensuring the reliability of the complete IoT network infrastructure [9].

To avoid these threats, the IoT must have strong security foundations built on a holistic view of security for all IoT elements at all stages -from the identification of objects to the provisioning of services, from obtaining of data to the governance of the whole infrastructure. All security mechanisms must consider each object’s lifecycle and services from the very beginning of that object’s existence [9].

Following are the challenges encountered by a developing IoT system:

Table 1 : Challenges of IoT system

CHALLENGES	DESCRIPTION	SOLUTION
Network protocol used and network security	Use of different interconnect technologies and reliability of network elements affects the quality of IoT network like putting together devices using low bandwidth standards like IEEE 802.15.4 and more powerful components [10]. Optimal cryptography algorithm is required to secure this channel and appropriate key management systems, also the Network security protocols used to interact with other networks like Internet.	Security and protection for Security and protection of the network can be ensured by using right tools like antivirus, anti-malware, firewalls, and intrusion prevention and detection systems and keeping them up-to-date.
Privacy of user data	Ensuring privacy of user data is a key challenge in IoT. IoT’s easy availability makes the data privacy an arduous task. Care must be taken to collect only the right data in a secured way without affecting the other services the user has access.	There are security protocols like IPsec, I PV6 protocol etc., that helps in reliable data transfer between IoT severs and clients. These security protocols provide encryption and authentication facilities to the valuable data. Advanced firewalls can be installed in each segment of an organization to provide complete protection from intruders.
Transparency	Sometimes the user would not know the entities they are managing. Hence they are denied of these access information and will face consequences.	The client and sever should come to an agreement which enforces a complete transparency between them. Client data should be used only for the indented purpose only and to be shared with others
Data handling and retrieval	Huge amount of data collected from various things leads to various challenges. Decides who manages the secrets and how. Traditional data management systems and algorithms cannot handle the huge amount of data. Generally, all the algorithms and methods	Data management policies must be developed. Latest big data related techniques and algorithms need to be incorporated to handle a large volume of data. Not only developing, but also implementing these rules properly is trivial.

	employed to protect the data for their life cycle poses problem in such mechanisms [11].	
Identity management	The IoT design lacks on distinguishing different objects based on its specification. Therefore the user finds it harder to locate and manage the object. An authorization problem also occurs due to identity mismanagement. Sometimes IoT cannot identify the deputed person and results in delayed process.	Proper description about the object should be provided with its dedicated ID (identification). A detailed information about the user is necessary to avoid authentication / authorization problems.
Trust and governance	Trust and governance is necessary to establish trust between various things. In IoT system trust management is essential to obtain trust from the user perspective The design of the IoT security system when not given by the service provider, a doubt rises within the customer and causes trust issues between them. Use of governance to monitor unintended actions of the user creates mistrust in the user feels they are controlled. This reduces the personal space for the workers and to solve problems it takes a lot of efforts and details.	Usage of governance framework to solve issues should be only on crucial times as it takes a lot of energy and time. It can be used only for the monitoring of the required particular details.
Fault tolerance	Certain IoT based objects are easily accessible, it is more vulnerable and malicious entities will take control over the objects. The fault tolerance is the ability of the system to do its intended function by adopting to the change in environment even in a limited way and in doing so, the system becomes more susceptible to new threats.	Monitoring and checking the system at regular intervals makes it easier to detect and prevent the errors. Advanced protection schemes can be introduced to increase the fault tolerance of the system.
Lack of Standardization	The digital transformation is at a fast pace. But the IOT implementation does not cope up with it. The challenges faced by IoT increases everyday and when the company's systems are not up to date, it faces many problems. When there is no proper standardization, security risks increases and the system becomes more prone to malware attacks.	Companies should set proper standards to cope up with the transformation. Government should enforce strict restrictions and policies.
Connectivity glitches	As more things are connected to IoT interlinking and communication process becomes complex. The maintaining of IoT system becomes more expensive when the number of users connected to it increases. Also the cloud based storage becomes more complex and expensive.	Better algorithms and cryptographic logics should be implemented to avoid the connectivity glitches.

Further, section 4 briefly enumerates about the future scope of IoT based systems and section 5 concludes the overall view of the paper.

IV. FUTURE SCOPE

IoT developments are growing rapidly around the world and the connectivity between things is becoming large. The paradigm of connectivity is now well beyond computers and smartphones as we see it moving towards smart homes, smart cities, smart farming and smart cars and many more. The emerging trends in IoT convince us to believe that the future homes and territories could be safer and environment friendly - not to mention smart [12].

The user's experience is getting transformed to enhance the way of life much more interesting and somehow, simpler. Some future improvements that can be done are:

A. Smarter cities

Smart cities include smart lighting, smart transport systems and smart metering for the usage of electricity and water. This type of technology integration includes the data collection from various sensors and analysis of data. Smart cities could contribute to climate change, and the rising sea levels and increasingly harsh weather events are some of the impact felt. But cities are also popular ground for IoT-based systems that enable urban life to be more attractive, like convenient and fast transportation systems, automated street lighting and energy efficient buildings.

IoT provides tremendous safety to the citizens of a city by continuously monitoring the nature and events happening in the city.

B. Cleaner water and air

The Public life could be positively influenced by Internet of Things. Cities suffering from chronic pollution are aided by installing sensor networks that raise alertsto residents whenever pollution levels are beyond safe zones. The sensors via Bluetooth transmits data to smartphones, enables creating real-time maps, displaying air pollution levels across the city.

C. Smarter agriculture

The challenge for the Farmers across the world is to reduce the consumption of water and fertilizers, to improve the yield or quality of their products and to cut waste. Microclimates across cropland could be tracked, the change in temperature and humidity could be monitored as perishable goods move from field to stock house to enable extending their shelf life and eliminate waste.

D. Cutting food waste

Every one third of food production every year is wasted or lost somewhere along the supply chain. That's huge and equals 1.4 billion tons of nutrition lost for a growing planet. The crop losses could be minimized with IoT and also could improve productivity.

E. Connecting patients

With the advent of modern medicines, the aging population is on the raise which lacks personal care due to mobility and migration of younger generation. This serious gap could be compensated by the Internet of Things which could transform the healthcare industry by helping doctors gain faster access remotely to patients' data. Wearable, sensor devices that are internet enabled track a patient's heart rate, pulse, or even blood pressure making them increasingly affordable, accurate and compact. While there is a debate over the mode of safely collecting, transmitting and usage of this data, wearable are one of the most promising IoT applications in healthcare.

F. Smart home automation

Smart homes will become as common as a smart phone with the pace of IoT growth. The ability to control the nature and working of the systems in home from a remote place makes it easier and fascinating for the users to use it extensively.

G. Connected Vehicles

A connected smart vehicle will be able to adapt, enhance and analyze its own operation, maintenance and the on board sensors and internet connectivity shall secure the comfort of passengers. IoT based smart cars provides promising and fascinating features such as autopilot , complete 3D car infotainment system that helps the user to visualize the environment and the system differently .Smart cars are being developed today that can detect whether the driver is intoxicated and is ready to drive.

V. CONCLUSION

According to Gartner, while enterprise will account for most the revenue, consumer applications will drive the number of connected things. Gartner estimated a steep increase in the number of connected things in the consumer sector from 2.9 billion in 2015 to over 13 billion in 2020.

In conclusion, our daily life will be facilitated by the Internet of Things in many areas; the predictions and decisions become more effective by obtaining information, storing and analyzing them as never before. The strategies and techniques applied in IoT were discussed in this paper. The IoT devices enable collection of huge information, and the storage of massive data is enabled by of cloud systems. Bringing benefit to the society with the help of these data still have unknown dimensions. IoT technologies are changing today's world and a big change will happen in coming years. However, the threats and risks discussed in this paper are undoubtedly a challenge for enterprises in the IoT section to provide efficient and safe service to protect the user data.

ACKNOWLEDGMENT

The wish to thank the management of the Kalasalingam Academy of Research and Education, India, TVS Sensing Solutions Private limited, India and Thigagarajar College of Engineering, India for their support in this research work.

REFERENCES

1. NIU Ling , Zhou Kou Normal University, Zhoukou 466001, China; Design of Remote data acquisition system based on Internet of Things
2. Charu C. Aggarwal ,IBM T. J. Watson Research Center Yorktown Heights, NY , Naveen Ashish ,University of California at Irvine Irvine, CA ,Amit Sheth ,Wright State University Dayton, OH,THE INTERNET OF THINGS: A SURVEY FROM THE DATA-CENTRIC PERSPECTIVE
3. JayavardhanaGubbi, RajkumarBuyya, SlavenMarusic, MarimuthuPalaniswami ,Internet of Things (IoT): A vision, architectural elements, and future directions .
4. Ala Al-Fuqaha, Senior Member, IEEE, Mohsen Guizani, Fellow, IEEE, Mehdi Mohammadi, Student Member, IEEE, Mohammed Aledhari, Student

Member, IEEE, and MoussaAyyash, Senior Member, IEEE ,Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications .M.Suresh, P.Saravana Kumar, Dr.T.V.P.Sundararajan,PG scholar, Department of ECE, Bannari Amman Institute of Technology, Sathyamangalam, TamilNadu, India. Assistant Professor (Sr. Grade), Department of ECE, Bannari Amman Institute of Technology, Sathyamangalam, TamilNadu, India;Data Security in IoT Environment

5. Qihui Wu, Senior Member, IEEE, Guoru Ding, Student Member, IEEE, YuhuaXu, Student Member, IEEE, ShuoFeng, Zhiyong Du, Jinlong Wang, Senior Member, IEEE, and Keping Long, Senior Member, IEEE Cognitive Internet of Things:A New Paradigm beyond Connection .
6. Rodrigo Roman, Pablo Najera, and Javier Lopez University of Malaga, Spain ;Securing the Internet of Things
7. Tobias Heer, Oscar Garcia -Morchon, Ren´e Hummen, SyeLoongKeoh, Sandeep S. Kumar, and Klaus Wehrle COMSYS Group, RWTH Aachen University, Germany and Philips Research, the Netherlands;Security Challenges in the IP-based Internet of Things.
8. Multimedia Systems for Sustainability (CITSEM), Technical University of Madrid (UPM), “La Arboleda-Campus Sur” Building, Crt. Valencia, Km. 7, 28031 Madrid, Spain,An Internet of Things Approach for Managing Smart Services Provided by Wearable Devices
9. Marko Bertogna, Nathan Fisher, and SanjoyBaruah ,Resource-Sharing Servers for Open Environments
10. Jatinder Singh, Thomas Pasquier, Jean Bacon, HajoonKo, and David Eyers Twenty security considerations for cloud-supported Internet of Things
11. Zhuming Bi, Senior Member, IEEE, Li Da Xu, Senior Member, IEEE, and Chengen Wang, Senior Member, IEEE ,Internet of Things for Enterprise Systems of Modern Manufacturing

AUTHORS PROFILE

Venkataraman Balaji is currently serving as President at TVS Sensing Solutions Private Limited. He received his B.E., and M.E degrees from Thiagarajar College of Engineering, Madurai, Tamilnadu, India in 1991 and 1997 respectively and pursuing Ph.D at Kalasalingam academy of Research and Education, India. His major areas of research interest are Strategy, Industrial Engineering, Industrial Internet of Things and Big Data.

Dr. P. Venkumar, is currently a Senior Professor in Department of Mechanical Engineering, Kalasalingam Academy of Research and Education, Krishnankovil, Tamilnadu, Inida. He received his B.E., and M.E., degrees in Thigagrajar College of Engineering, Madurai, Tamilnadu, India, in 1994 and 1997, respectively and Ph.D. degree in Manonmaniam Sundaranar University, India in Industrial Engineering in 2006. His main areas of research interest are manufacturing system optimization, Supply chain management and Smart manufacturing

Dr. M. S. Sabitha is serving as Head, Information Systems at TVS Sensing Solutions Private Limited.She received her B.Sc and M.C.A from Madurai Kamaraj Univeristy in 1994 and 2000 respectively. M.Phil from Alagappa University in 2004 and Ph.D from Bharathiar University in 2019. Her main areas of research interest are Big data, Data mining and Internet of things.

Dr. S. Vijayalakshmi is serving as an Associate professor at Thiagarajar College of Engineering. She received her M.Com from Madurai Kamaraj University in 1991 and M.C.A from Thiagarajar College of Engineering in 1994. M.Phil from Madurai Kamaraj Unveristy in 2004. Ph.D in Computer Science from Anna University in 2011. Her main areas of research interest are Big data and Data mining.