IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

Internet of Things: Challenges and Privacy Issues

Sapna Sharma[1] and Dr. Shikha Lohchab[2]
Research Scholar, Department of Computer Science and Engineering[1]
Assistant Professor, Department of Computer Science and Engineering[2]
G D Goenka University, Gurugram, Haryana, India

Abstract: *The recent trends in the field of Computer Engineering shows that The Internet of Things (IoT) has gained lots of popularity among the researchers. Internet of things (IoT) is simply the virtual representation of any kind of objects, things, systems by means of allocation of unique identification systems and internet . IoT works on many kinds of internet Connections such as: RFID, Wi-Fi, Bluetooth, and ZigBee, in addition to allowing wide area connectivity using many technologies such as GSM, GPRS, 3G, and LTE. This study is focused on the literature survey in the area of IoT; to identify the advancement and achievement in the field of IoT; to identify any limitation, pothole associated with this technology; to identify possible solutions and methods to overcome the limitation. At the end, this study gives more emphasis on solving the security issue associated with IoT and suggests that proper steps have to be taken in the initial phase itself before going for further development of IoT. This will turn the IoT into an effective and widely accepted and adopted technology in near future.*

Keywords: IOT, RFID, WSN, DoS

I. INTRODUCTION

Idea for IoT was proposed by Kevin Ashton in 1982 with the intention of providing an advanced mode of communication between various systems & devices as well as to facilitate the interaction of humans with the environment[1]. In the past 36 years, applications of IoT have been implemented in various fields viz; Smart devices, Smart phones, Smart cars, Smart homes, Smart cities, a smart world and research communities are mainly focused in the field of Internet of Things (IoT), Mobile Computing (MC), Pervasive Computing (PC), Wireless Sensor Networks (WSN), and most recently, Cyber Physical Systems (CPS) [2].

1.1 History of IoT

- Late 1960: Communication between two computers was possible through a computer network.
- Early 1980: TCP / IP stack was introduced.
- Late 1980: Commercial use of the Internet started.
- 1991: World Wide Web (www) introduced which made the internet more popular and created the path for rapid growth.
- Recently mobile devices connected to the internet (Mobile Internet).

In 1999, MIT Auto-ID Labs first proposed the concept of the Internet of Things, which investigated object localization and state recognition using wireless sensor networks and radio frequency identification technologies [3]. In 2005, International Telecommunication Union (ITU) proposed the concept of the Internet of Things and reported that IoT can exchange information via the networks [4]. In 2009, IBM presented the‖ Smart- Planet‖ concept which aims to embed sensors in several physical objects such as power grid, railway, buildings, and make them smart by intelligent processing technologies [5]. The IoT is empowered by the latest developments in RFID, smart sensors, communication Technologies and Internet protocols. The current rebellion in mobile, machine-to-machine (MZM) and Internet technologies can be seen as the first stage of the IoT [6]. By the end of 2020 it is said that there would be around 50 billion connected devices [l]. The data exchanged over the network will be greater than 40 Zettabytes for the same period [7], [18].

1.2 IoT Overview

IOT is used to exchange information between two or more devices, nodes, system automatically without the presence of any kind of manual input. For this purpose, IoT uses some communication technologies like Wireless Sensor Network

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

(WSN) and Radio Frequency Identification (RFID) [5], [7], [9]. The communicating node of a typical wireless sensor network consists of Sensor, Microcontroller, Memory, Radio transceiver, Battery.

Tuhin Borgohain et al. (2015) investigated WSN are compositions of independent nodes whose wireless communication takes place over limited frequency and bandwidth whereas RFID tags use radio frequency waves for interacting and exchanging information [5]. RFID is made up of RFID tags (transponder) and RFID readers (Transceiver). As per classification the two types of RFID tag areas mentioned as: Active Tag: Tag has a battery internally which facilitates the interaction of unique EPC (electronic product code) with its surroundings remotely from a limited distance. Passive Tag: The lack of an internal battery in the passive tag is substituted by its utilization of external sources of energy [5], [6].

IoT= Internet + WSN + Smart Items surrounded by Intelligent environment

1.3 IoT Architecture

The security of information and network should be equipped with these properties such as identification, confidentiality, integrity and undeniability [10]. Different from internet, the IoT will be applied to the crucial areas of national economy, In general, the IoT can be divided into four key levels [6], [8], [9], Fig.1 shows that the level architecture of the IoT .

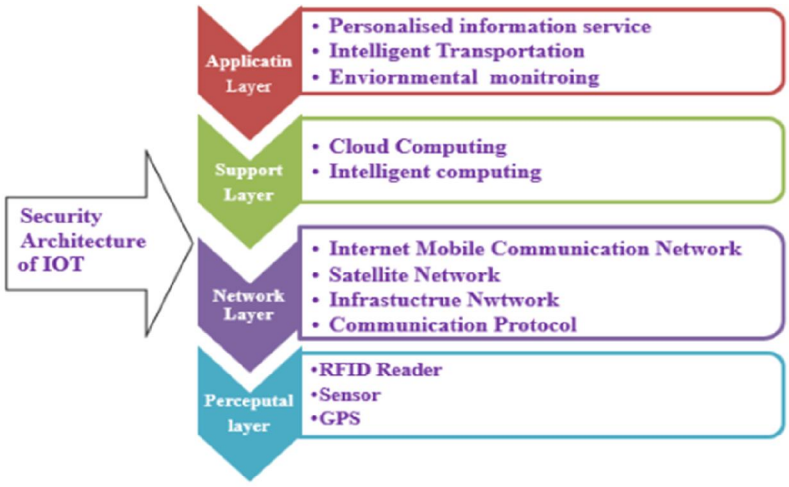

Figure 1. Security Architecture of IOT

- **Perceptual Layer:** The perception layer is also known as the ―Sensors‖ layer in IoT. The most basic level is the perceptual layer (also known as recognition layer), which collects all kinds of information through physical equipment and identifies the physical world, the information includes object properties, environmental all kinds of sensors, GPS and other equipment ‘s. The key component in this layer is sensors for capturing and representing the physical world in the digital world [12], [13].
- **Network Layer:** The network layer of IoT serves the function of data routing and transmission to different IoT hubs. It is responsible for the reliable transmission of information from perceptual layer, initial processing of information, classification and polymerization [12], [13].
- **Support Layer:** It will set up a reliable support platform for the application layer, on this support platform all kind of intelligent computing powers will be organized through network grid and cloud computing. It plays the role of combining application layer upward and network layer downward.
- **Application Layer:** The application layer is the topmost and terminal level. It provides personalized services according to the needs of the users. Users can access the internet of thing through the application layer interface using television, personal computer or mobile equipment and so on. Network security and management play an important role above each level. Then we will analysis the security features

II. LITERATURE REVIEW

Rwan Mahmoud, Tasneem Yousuf, et al. (2015) investigated that in spite of the immense potential of IoT in the various spheres, the whole communication infrastructure of the IoT is flawed from the security and is susceptible to loss of privacy

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

for the end users. The security challenges of IoT can be broadly divided into two classes; Technological challenges and Security challenges [7]. The technological challenges arise due to the heterogeneous and ubiquitous nature of IoT devices, while the security challenges are related to the principles and functionalities that should be enforced to achieve a secure network. Technological challenges are typically related to wireless technologies, scalability, energy, and distributed nature, while security challenges require the ability to ensure security by authentication, confidentiality, end-to-end security, integrity etc. [7], [9], [10].

Dr. Anju (2017) investigated the hierarchical relationship of the various security issues plaguing the wireless sensor network. She categorized the oppressive operations which can be performed in a wireless sensor network as (a) Attacks on secrecy and authentication (b) Silent attacks on service integrity (c)attacks on network availability [17, 18, 19].

Diego Mendezl (2018) has also determined security requirements for the Internet of Things, which include: (a) attack resiliency (b) data authentication, (c) access control, and finally demand (d) client Privacy. He also proposes that security requirements to protect IoT data transmission, which include the following: (a) key management, (b) appropriate secret key Algorithms, (c) secure routing protocols, (d) intrusion detection technology, (e) authentication and access control, and finally, (t) physical security design [18]

According to [20, 21] the denial of services attacks (DoS) in the WSN devices falls under the category of attack on availability can occur on different layers of the network including DoS attacks on the physical layer (jamming, node tampering), DoS attacks on the link layer (collision, unfairness, battery exhaustion), DoS attacks on the network layer (spoofing, hello flood, homing, selective forwarding, Sybil, wormhole acknowledgement flooding), DoS attacks on the transport layer (flooding, de-synchronization) and DoS attacks on the application layer (traffic congestion generation).

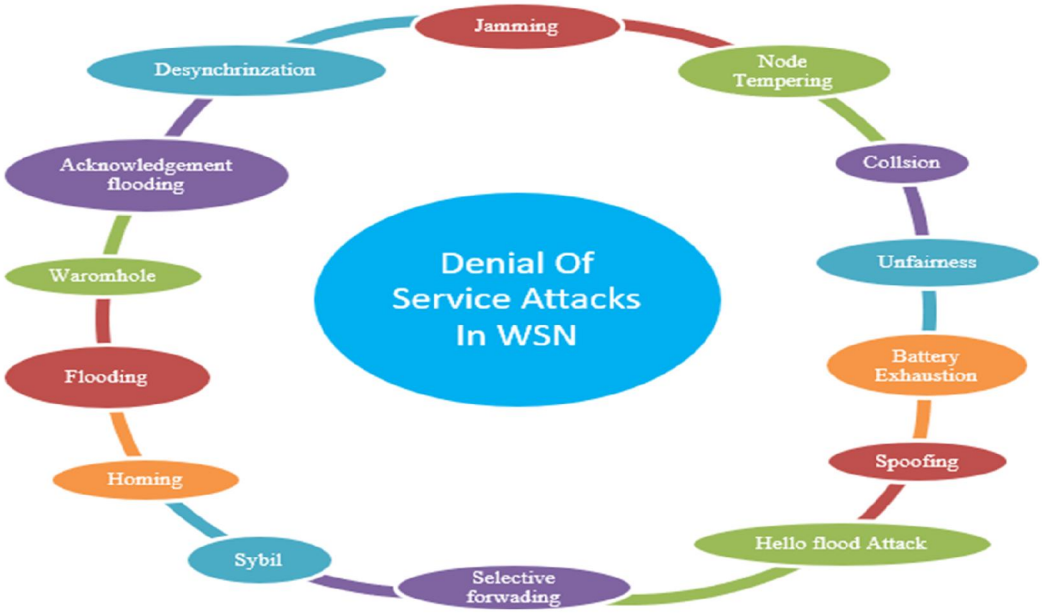

Figure 2. Denial of Service Attack in Wireless Sensor Network.

He then furthers categories attacks on WSN as: (a) external, (b) internal, (c) passive, (d) active, (e) mote-class, (f) laptop class, (g) interruption, (h) interception, (i) modification, (j) fabrication, (k) host-based and (1) network based [23].

According to [22, 23] due to the security vulnerabilities in the systems can lead to user dissatisfaction (for instance, random bugs), privacy violation (for instance, eavesdropping), monetary loss (for instance, denial-of service attacks or ransom are), or even loss of life (for instance, attackers controlling vehicles).their work focus on two themes; 1. Security for hardware and hardware for security; 2 System Software Layer: The system software layer consists of firmware, OS code, and any privileged system applications or programming frameworks. This layer we believe that many security principles developed in the context of mobile, desktop, and cloud computing will be applicable to IoT platforms.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

III. IoT Security Issues

Literature review shows that most of the systems, objects, technologies, virtual systems and many other things are widely using the internet infrastructure for information exchange, due to this; IoT is susceptible to various security issues and has some major privacy concerns for the end users. Thus, this study gives more emphasis on solving the security issue associated with IoT.

- **Identity Management**: Proving identity is an important part of identity management. As developers create a worldwide network of objects, they must build an infrastructure that allows mutual object authentication. There must be a balance between centralized management and a distributed, hierarchical approach [14].
- **Protocol and Network Security**: Securing this channel requires optimal cryptography algorithms and adequate key management systems, as well as security protocols that connect all these devices through the Internet [10,15]
- **Heterogeneity:** greatly affects the protection of the network infrastructure. Highly constrained devices that use low-bandwidth standards, such as IEEE 802.15.4, must open a secure communication channel with more powerful devices—for example, sensor nodes scattered in a smart city communicate with smart phones or PDAs [11].
- **Optimize Security:** Although, it is not clear how many resources will be available to such constrained devices once the IoT truly takes off, it is safe to optimize security as much as possible to improve the provision of future services.
- **Key-Management**: Cryptographic mechanisms must be smaller and faster but with little or no reduction in security level. Mechanisms could include symmetric algorithms, hash functions, and random number generators cryptography is the bricks and the mortar is the key-management infrastructures that establish keying material, for example, shared secret keys [16].
- **Data and Privacy**: Privacy is one of the most sensitive subjects in any discussion of IoT protection. The data availability explosion has created Big Brother-like entities that profile and track users without their consent. The IoT ‘s anywhere, anything, anytime nature could easily turn such practices into a dystopia [11].
- **Privacy by Design**: One viable solution is privacy by design, in which users would have the tools they need to manage their own data [12].
- **Transparency:** Transparency is also essential, since users should know which entities are managing their data and how and when those entities are using it.
- **Data Management**: A huge issue is deciding who manages the secrets. Technically, cryptographic mechanisms and protocols protect data throughout the service ‘s life cycle,
- **Trust and Governance: Trust** is essential to implement the IoT. In this context, trust is more than the mechanisms that reduce the uncertainty of objects as they interact, Governance helps strengthen trust in the IoT. A common framework for security policies will support interoperability and ensure security ‘s continuity.
- **Fault Tolerance** clearly, the IoT will be more susceptible to attack than the current Internet, since billions more devices will be producing and consuming services

IV. IoT Challenges and Privacy Concern

IoT as a very active and new research field, a variety of questions need to be solved, at different layers of the architecture and from different aspects of information security.

- Challenge 1: The need for a comprehensive understanding of the complete spectrum of types of human-in-the-loop controls.
- Challenge 2: The need for extensions to system identification or other techniques to derive models of human behaviors.
- Challenge 3: Determining how to incorporate human behavior models into the formal methodology of feedback control.

In this section problems and required research are highlighted in 8 topic areas: massive scaling, architecture and dependencies, creating knowledge and big data, robustness, openness, security, privacy, and human-in-the-loop [20]. A Framework to detect Denial of Service (DoS) attacks in IoT will be proposed and its effectiveness will be measured. There is currently no single standard protocol in IoT. The protection of data and privacy of users has been identified as one of the key challenges in the IOT. Everything is connected in the local network and can communicate freely with one another. Connections to the internet are directed through the central router, which may contain basic firewall filtering functionality

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

V. CONCLUSION

The IoT is highly distributed in nature and promises to extend ―anywhere, anyhow, anytime‖ computing to ―anything, anyone, any service. However, without strong security foundations, attacks and malfunctions in the IoT will outweigh any of its benefits. Existing traditional protection mechanisms such as cryptography, secure protocols, and privacy assurance are not enough. In the future IoT will become a utility with increased sophistication in sensing, actuation, communications, control, and in creating knowledge from vast amounts of data. This will result in qualitatively different lifestyles from today. It would be fair to say that we cannot predict how lives will change. We did not predict the Internet, the Web, social networking, Facebook, Twitter, millions of apps for smartphones, etc., and these have all qualitatively changed societies ' lifestyles. New research problems arise due to the large scale of devices, the connection of the physical and cyber worlds, the openness of the systems of systems, and continuing problems of privacy and security.

At the end, it is suggested that the proper legal and technical framework is essential and has to be taken in the initial phase itself before going for further development of IoT so that it will be effectively and widely accept and adopted in near future.

ACKNOWLEDGMENT

- **Funding**: This research received no external funding
- **Conflicts of Interest:** The authors declare no conflict of interest.

REFERENCES

[1]. R. H. Weber, ―Internet of things – new security and privacy challenges, ‖ Computer Law & Security Review, vol. 26, pp. 23-30, 2010.

[2]. John A. Stankovic, Life Fellow, "Research Directions for the Internet of Things‖ IEEE Internet of Things Journal (Volume: 1, Issue: 1, Feb. 2014)Pp. 3 – 9,Mar 2014.

[3]. I. Bose and R. Pal, ‖Auto-ID: managing anything, anywhere, anytime in the supply chain‖, Communications of the ACM, vol. 48, No. 8, pp. 100-106, Aug. 2005.

[4]. ITU, ‖ITU Internet Reports 2005: The Internet of Things‖, The Internet of Things, Nov. 2005.

[5]. S. Sanyal , T. Borgohain, U. kumar, University of Louisiana at Lafayette online: ―Survey of Security Issues And Privacy Of Internet Of Things. Available :Research gate online

[6]. , https://www.researchgate.net/publication/270763270 2015 [Accessed:Feb4,2015].

[7]. Hui Suo, JiafuWana, IEEE computer society ,International Conference on Computer Science and Electronics Engineering, ―Security in the Internet of Things: A Review‖ 978-0- 7695-4647-6/12 © 2012 IEEE, DOI 10.1109/ICCSEE.2012.373.648.

[8]. Rwan Mahmoud, Tasneem Yousuf, et al.. Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures‖ IEEE Published in: Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for DOI: 10.1109/ICITST.2015.7412116.

[9]. Z. Kamal, A. Mohammeda, E. Ahmed, "Internet of Things Applications, Challenges and Related Future Technologies." https://www.researchgate.net/publication/313651150 Article: January 2017.Available online at www.worldscientificnews.comWSN 67(2),pp 126-148, 2017.

[10]. Qian Zhu, Ruikang Wang, Yan Liu, "IOT Gateway: Bridging Wireless Sensor Networks into Internet of Things Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on Date of Conference: 11-13 Dec. 2010, DOI: 10.1109/EUC.2010.58

[11]. Q. Liu, L. Cui, HM. Chen, ‖Key technologies and applications of Internet of Things‖, Computer Science, Vol. 37, No. 6, 2010.

[12]. Carsten Maple ,‖Security and privacy in the internet of things‖ Article · May 2017 DOI: 10.1080/23738871.2017.1366536

[13]. C. suchitra , vandana, "Internet of Things and Security Issues‖, IJCSMC, vol. 5, Issue. 1, January 2016, pg 133-139 .

[14]. J. Sathish Kumar, Dhiren R. Patel, ―A Survey on Internet of Things: Security and Privacy Issues‖ International Journal of Computer Applications (0975 – 8887) vol. 90 – No11, March 2014.

[15]. MB Barcena, ‖Insecurity in the Internet of things-Symantec", https://www.symantec.com, Nov 2014.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

[16]. Rodrigo Roman, Pablo Najera, and Javier Lopez, ―Securing the Internet of Things‖, IEEE Published in: Computer , vol. 44, Issue: 9, Sept. 2011, Page(s): 51 – 58.

[17]. The Internet of Things: Security research study veracode https://www.veracode.com/sites/.../Whitepapers /internet-of-things-whitepaper.pdf.

[18]. Dr Anju Bhandari Gandhi, Jeetkaur, ―Security and Ddos Mechanisms in Internet of Things‖, International Journal of Advanced Research in Computer Science ISSN No. 0976- 5697 DOI: http://dx.doi.org/10.26483/ijarcs.v8i9.5008

[19]. Diego Mendez, Ioannis Papapanagiotouz, Baijian Yang, ‖ Internet of Things: Survey on Security and Privacy‖ Information Security Journal: A Global perspective (2018) DOI: 10.1080/19393555.2018.1458258 https://arxiv.org/abs/1707.01879

[20]. Earlence Fernandes, Amir Rahmati, Kevin Eykholt, and Atul Prakash, ―Internet of Things Security Research: A Rehash of Old Ideas or New Intellectual Challenges?‖ IEEE Security & Privacy, vol.15, Issue 4, 2017, Page(s): 79 - 84 INSPEC Accession Number: 17121924 DOI: 10.1109/MSP.2017.3151346.

[21]. Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li and Hongbin Zhao,‖ A Survey on Security and Privacy Issues in Internet-of-Things‖, IEEE Internet of Things Journal, vol. 4, Issue 5, Oct. 2017, Page(s): 1250 – 1258, Date of Publication: 17 April 2017 INSPEC Accession Number: 17281982 DOI: 10.1109/JIOT.2017.2694844

[22]. Pratiksha Gautam, AP Goyal, "A Review on Internet of Things‖ AGU International Journal of Engineering & Technology (AGUIJET) 2018, vol. 7, Jul-Dec e-ISSN: 2455-0442, p-ISSN: 2455-6734 http://www.aguijet .com.

[23]. Mauro Conti1, Ali Dehghantanha , Katrin Franke, Steve Watson, "Internet of Things Security and Forensics: Challenges and Opportunities", Future Generation Computer Systems vol. 78, 2018, 544-546, Journal homepage: www.elsevier.com/locate/fgcs

[24]. Nikita Chaudharil, Amit Palve, "Securing Real time data in IoT Environment", International Journal of Research in Advent Technology, vol.6, No.6, June 2018 E-ISSN: 2321-9637 www.ijrat.org

[25]. Stephen Cobb 10 things to know about the October 21 IoT DDoS attacks.

BIOGRAPHY

Sapna Sharma received BE in Computer Science and Engineering from Amravati University, India in 1997, MTech in Computer Science from IETE, New Delhi, India. She worked as lecturer in Border Security Force STS-1, New Delhi and has a rich experience of 21 years. Prior to that she worked at Hitkarini College of Engineering and Technology Jabalpur and Government college of Engineering, Jabalpur. Her research interests include biometric security, personal authentication, image processing, machine learning, and deep learning.
Email: sapnaloksharma@gmail.com.

Dr. Shikha Lohchab is a Researcher with a background in Wireless Sensor Network. She is an expert with comprehensive knowledge of both Mobile Adhoc Network and Wireless Sensor Network, Technique Characterization of components by Dynamic Topologies, Bandwidth Constraints, Autonomous behavior, Limited Security etc. Shikha Lohchab has teaching experience of 6 years and prior to joining G D Goenka University, she joined as an Assistant professor at DPG Group of Institution, Gurugram. She completed her BE studies in Kurukshetra University and the Post graduate in Amity University.
Email: Shikha.lohchab@gdgu.org.