International Interdisciplinary Virtual Conference on
'Recent Advancements in Computer Science, Management and Information Technology'
International Journal of Scientific Research in Computer Science,
Engineering and Information Technology| ISSN : 2456-3307 (www.ijsrcseit.com)

A Study on Security and Privacy Challenges in the Internet of Things

Ghanshyam G. Parrkhede[1], Akshay Dilip Lahe[1], Bhushan L. Rathi[1]
[1]Assistant Professor
Saraswati College, Shegaon, Maharashtra, India

ABSTRACT

Wireless communication is used to remotely control devices in IoT systems, making them vulnerable to attacks from hackers and cybercriminals. IoT devices collect vast amounts of personal and sensitive data, which can be accessed by unauthorized entities, facing the problems of privacy and security. In recent year "Internet of Things" is research attention for wireless network. The term IoT stands for "Internet of Things", referring to the interconnectivity of objects to the internet, allowing them to access it. The potential for IoT is vast, with billions of devices, people, and services able to exchange information and useful data in various locations worldwide.

IoT used in healthcare, homes automation, business, company, military purpose, for wireless communication and control the environments. In IoT "things" are connected to web each device has unique ID for verification. In future electronic devices will be smart which can be communicating with other devices and other system. IoT required very accurate and consistence, integrate data for accessing system and control the system. The Internet of Things (IoT) has brought to light a number of security and privacy issues that need to be addressed. Security and privacy are the main concerns in IoT, and they require attention to areas such as identification, verification, authentication, and device diversity for real protection.

In this paper, the vision of IoT, existing security threats and open challenges, as well as security requirements in the domain of IoT are discussed, with basic issues identified in relation to the safety and privacy of IoT.

Keywords: Internet of things, Information security, security & Privacy in IoT, verification & identification

Introduction

I. INTRODUCTION

IoT means "Internet of things "the object is connected to internet and accesses it. In IoT everywhere. Billions of devices, people & services to be interconnected for exchange information and useful data.

IoT means "The internet of things" means interconnection of thing-to-thing to internet that is also called as networks of sensors. which are embedded with sensor, software, electronics devices and network connectivity that help to retrieve and exchange the information In IoT there is advanced connectivity among the electronic device and system. In that all things are connected to the internet with strong connectivity that gives machine-

to-machine relation means they can exchange the information, and they can communicate without human interaction or without human instruction.

The overall IoT context will consist of billions of individuals, individual devices, and services that can interconnect to exchange data and useful information [1].

Because of quick headways in portable correspondence, Wireless Sensor Networks (WSNs) and Radio Frequency Identification (RFID) advancement, things and systems in IoT can possibly work together with each other whenever, anyplace and in any structure There are numerous conceivable application territories on account of these brilliant things or articles. The major IoT target is simply the arrangement of shrewd situations and cognizant/self-sufficient gadgets: keen vehicle, savvy things, brilliant urban areas, savvy wellbeing, shrewd living, etc As far as business, IoT speaks to the enormous possibility for various sorts of associations, including IoT applications and specialist co-ops, IoT stage suppliers and integrators, telecom administrators and programming sellers Many vertical segments are expected to experience a double-digit growth in upcoming years. Among the most prospective vertical application domains are consumer electronics, automotive industries, and healthcare, as well as intelligent buildings and utilities. With the rapid increase in IoT application use, several security and privacy issues are observed. When nearly everything will be connected to each other, this issue will only become more pronounced, and constant exposure will literally reveal additional security flaws and weaknesses. Such limitations may subsequently be exploited by hackers, and in a statistical sense all exposed flaws and weaknesses may be abused in an environment with billions of devices [9]. Be that as it may, without strong security set up, assaults and glitches in the IoT may exceed any of its advantages.

Scalability factors and various restrictions on device capabilities also mean that traditional cryptography mechanisms, security protocols, and protection mechanisms are unavailable or insufficient [11]. The baseline security must be robust and the security architecture must be designed for long system life cycles (>20 years), something indeed challenging. Dealing with large device populations further makes it understandable that some devices will be compromised. Therefore, new methodologies and technologies ought to be developed to meet IoT requirements in terms of security, privacy and reliability [12].

The rest of the paper is organized as follows. In section this section introduction and overview of the IoT. In section II vision of IoT, section III application of IOT in various areas. Section fourth identifies some of the IoT security challenges and describes the security requirements in the IoT. Finally, in section and the paper is concluded.

II. THE VISION OF IOT

The IoT vision is to revolutionize the Internet, to create networks of billions of wireless identifiable objects and devices, communicating with each different anytime, anyplace, with anything and each person using any service. The growing greater processing competencies of RFID technologies, wireless sensor networks (WSNs) and storage potential at decrease cost may create a pretty decentralized frequent pool of resources interconnected by a dynamic gadget of networks Through IoT architecture, intelligent middleware will be capable of creating dynamic maps of the physical world within the digital/virtual sphere by applying high temporal and spatial resolution and combining the characteristics of ubiquitous sensor networks and other identifiable things. Figure 1 shows the symbiotic interaction among the real/physical, digital, and virtual worlds with society [14].

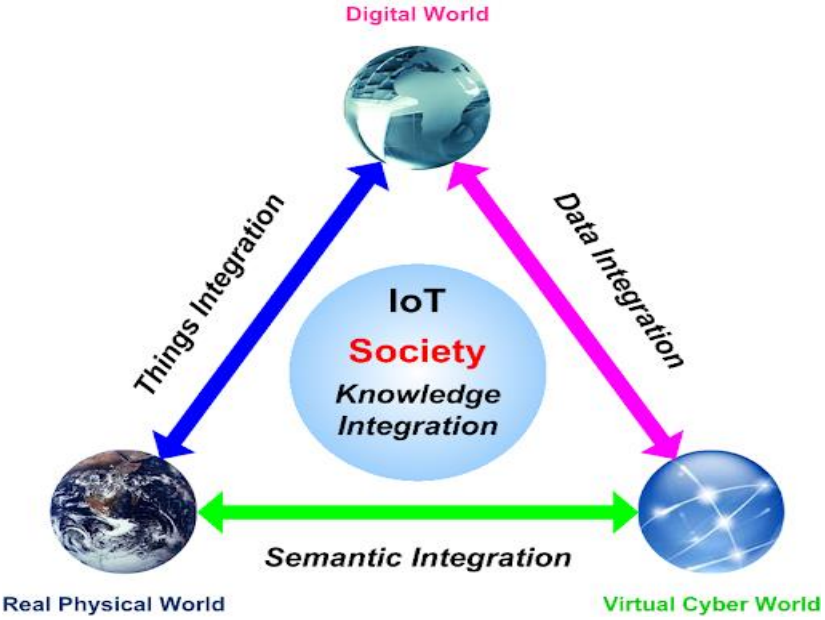

Fig 2. Internet of Things –a symbiotic interaction among the real/physical, the digital, virtual words & society [13]

In fact, communications in the IoT will take place not only between devices however additionally, between humans and their environment as introduced in Figure 2. All man or woman objects of our everyday existence such as people, vehicles, computers, books, TVs, cell phones, clothes, food, medicine, passports, luggage, etc., will have at least one special identification allowing them to correspond with one another.

Besides, since these articles can detect the earth, they will have the capacity to confirm personalities and speak with each other, with the end goal that they will have the option to trade data furthermore, become implies for getting unpredictability, and may regularly empower autonomic reactions to troublesome situations without human contribution

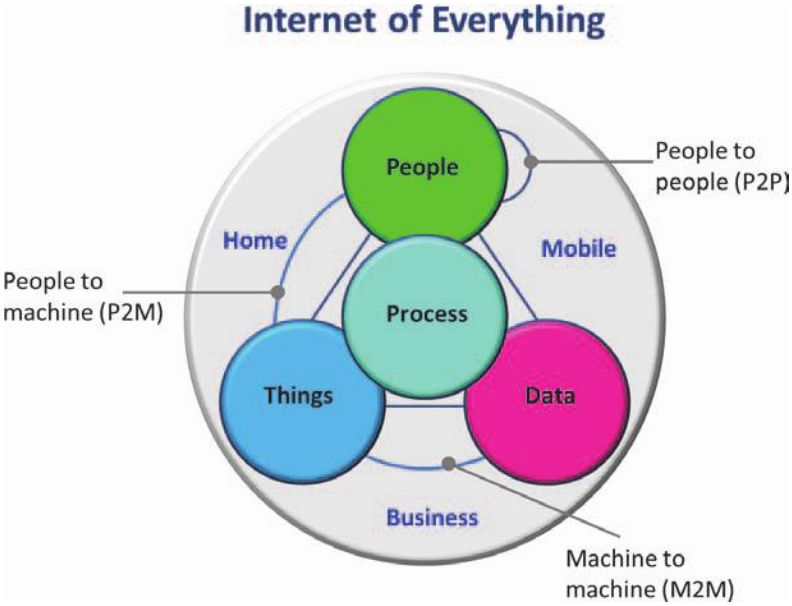

Fig. 2. Internet of Everything [17]

III. APPLICATION OF IOT IN VARIOUS AREAS

The primary goal of IoT are simply the arrangement of a keen domain and hesitant autonomous gadgets, for example, savvy living, brilliant things, shrewd wellbeing, and keen urban communities among others The applications of IoT in various areas example industries, medical field, and in home automation are discussed in the following section.

1. IoT in Industries

The IoT has given a sensible opportunity to amass enormous present-day structures and applications in an adroit IoT transportation system, the endorsed individual can screen the Existing territory and improvement of a vehicle. The affirmed individual can in like manner predict its future zone and road traffic. In the earlier stage, the term IoT was used to remember one of the kind items with RFID. Up to this point, the researchers relate the term IoT with sensors, Global Positioning System (GPS) devices, mobile phones, and actuators. The affirmation and organizations of new IoT developments mainly depend on the insurance of data likewise, the security of information. The IoT licenses various things to be related, followed and checked so significant information likewise, private data assembled, therefore. In IoT condition, the security affirmation is an inexorably essential issue when stood out from traditional frameworks since the amounts of attacks on IoT are high.

2. Personal & Social Domain

The applications falling in this category permit users to interact with their surroundings (home and work) or with other people to maintain and build social relationships [2]. IoT application in smarts cars smart homes smart cities for security purpose. IoT gadgets are a piece of the bigger idea of home mechanization, which can incorporate lighting, warming and cooling, media and security frameworks. Long haul advantages could incorporate vitality investment funds via naturally guaranteeing lights and hardware is killed

3. IoT in Medical

The Internet of things day by day use in medical & health care sector both doctor & patient example Thermometer, ECG, ultrasound also tracking patient for his health.

Kaa is an open-source IoT middleware stage for overseeing, gathering, breaking down, and following up on each part of correspondences between associated devices. Kaa offers a scope of pluggable elements that permit building killer applications for purchasing items in days rather than weeks. Out of the box, Kaa is perfect with basically any present-day customer object or microchip — smart TVs, brilliant home appliances, HVAC frameworks, wearable, and smaller scale PC boards [13].

4. IoT in Education system

In recent days, many schools and colleges used advance technology for their working. when we use advanced technology in education system automatically improve the quality of education in schools and colleges. Education is need of an hour in education system consists three main components which are students, faculties and parents, these three components perform important role in education system without their communication the system will become fail. Implementation of IoT in student's attendance smarts teaching, smart Library

management using IoT, display information on notice boards and class room management. This system improves the quality of education standardized management.

5. IoT in Smart Cities

Savvy city is another incredible utilization of IoT producing interest among total populace. Keen reconnaissance, robotized transportation, more intelligent vitality the board frameworks, water conveyance, urban security and ecological checking all are instances of web of things applications for savvy urban communities.

IoT will take care of serious issues looked by the individuals living in urban communities like contamination, traffic blockage and deficiency of vitality supplies and so on. Items like cell correspondence empowered Smart Belly garbage will send alarms to city administrations when a container should be purged.

By introducing sensors and utilizing web applications, residents can discover free accessible stopping openings over the city. Additionally, the sensors can recognize meter altering issues, general breakdowns and any establishment issues in the power framework.

IV. KEY CAHLLENGES FOR SECURITY AND PRIVACY OF IOT

We will continue with a presence where people are by all account not the only data creators anyway the things that are furnished with appropriate fragments will make data. As needs be, this decade is foreseen to see the ascent of related gadgets that are not cell telephones and don't require human control. Along these lines, we need a critical structure for impeccable convenience. Specialized issues of IoT join Energy, Wireless correspondence, Scalability, Security, etc. Here are some security related issues in IoT.

Object Identification:

Validation in IoT is perhaps the best issue because of the quantity of gadgets. Confirmation for each and every contraption is definitely not a solitary occupation to wrap up. On account of the components of speedy figuring and essentialness profitability, considering private key cryptographic natives, various security strategies have been proposed

Authentication

Verification in IoT is probably the best issue because of the quantity of gadgets. Confirmation for each and every contraption is certifiably not a solitary occupation to wrap up. In light of the components of snappy computation and essentialness profitability, considering private key cryptographic natives, various security strategies have been proposed.

Data Management

Conspicuous evidence of billions of gadgets and their sending can be seen as an essential issue in IoT. As showed by estimations, constantly 2020 in excess of 50 billion gadgets will be related with the web. Managing the gadgets and their sending will be inconvenient despite for IPv6.There is strategies that can be used for conspicuous verification of the things in IoT. Some of them are Bar code recognizable proof, vision-based item distinguishing proof, etc. RFID and NFC developments are used for separating purposes.

Heterogeneity

The greatest security and protection issue is by a long shot the problem of device heterogeneity. Issues should be handled appropriately to make IoT more secure and robust. Administering hundreds of distinctive sorts of devices with each has their own security problems and necessities. Each object should be handled contrastingly which makes it hard to apply a single resolution to all. It will be an extreme assignment to secure each sort of the device from various kinds of incidents. It makes it harder to supervise the items. Every device imparts and works distinctively when contrasted with other objects. Device heterogeneity can influence numerous different perspectives also, for example, trouble in combination, security, and distinguishing proof and so on [15].

Data Secrecy & encryption

The sensor devices perform autonomous detecting or estimations and exchange information to the data handling unit over the transmission framework. It is vital that the sensor devices ought to have legal encryption instrument to ensure the information uprightness at the data preparing unit. A large number of devices associated with the web. So it would be hard to distinguish if any unapproved device associates with a current system and capture the critical data during an exchange over the internet. So confidentiality can be considered as the greatest test for the sake of security [16].

Bulk Data

Data is the essential factor in Internet of Things. IoT associates different machines with cloud server farms, in the cloud all devices are associated with cloud models and stores and recover a huge amount of information and data to cloud data centres. It would be tough to deal with all data centres as they are composed in dispersed condition and furthermore hard to deal with and keep up server farms in the request to store critical and private information [17].

Objects Safety and security

The IoT comprises of a huge number of perception objects that spread over a few geographic zones; it is important to keep the intruder's access to the items that may make physical harm them or may change their operation [14].

Connectivity of Internet

Web of Things partner’s different keen gadgets through the Internet, and it gives an office to concentrated checking and control of related gear. Along these lines, Internet of Things is only possible with the help of persistent web administrations and in the event that there is any issue, at that point it should in a flash be settled else it welcomes progressively extreme issue in the framework without the help of dynamic gadget.

Data Collection

One of the biggest privacy concerns with IoT is the vast amount of data that is collected by devices. This data can include personal information such as name, address, and credit card details, as well as behavioural data such as location, browsing history, and search queries. To protect privacy, IoT devices should only collect data that is necessary for their intended purpose. Organizations should also be transparent about the data they collect and how it will be used.

Data Sharing

Another privacy concern with IoT is the sharing of data between devices and organizations. Third-party organizations may gain access to personal information without the knowledge or consent of the user. To address this issue, IoT devices should be designed to limit data sharing and to provide users with control over the sharing of their data. Organizations should also have clear policies for data sharing and obtain user consent before sharing any personal information.

Security

Security is a critical aspect of IoT privacy. If IoT devices are not adequately secured, hackers can gain access to personal information, including sensitive data such as financial information and medical records. To protect privacy, IoT devices should be designed with robust security features, including data encryption, access control, and authentication.

User Control

User control is an essential aspect of IoT privacy. Users should have control over the data collected by IoT devices, including the ability to delete or modify their data. IoT devices should also provide users with clear and concise information about how their data is collected, used, and shared.

Transparency

Transparency is key to ensuring IoT privacy. Organizations should be transparent about the data they collect, how it will be used, and who it will be shared with. IoT devices should also be designed to provide users with clear and concise information about data collection, usage, and sharing.

V. SECURITY REQUIREMENT FOR IOT

IoT has gotten one of the most critical components of things to come to the Internet with a tremendous effect on public activity and Business Environment. As talked about in section-3 a bigger number of IoT applications and administrations are progressively powerless against assaults or data burglary. To verify IoT against such assaults, trend setting innovation is required in a few regions.

All the more explicitly, verification, classification, and information honesty are the key issues identified with IoT security. Verification is important for making an association between two gadgets and the trading of some open and private keys through the hub to forestall information robbery. Secrecy guarantees that the information inside an IoT gadget is avoided unapproved elements.

Information uprightness forestalls any man-in-the-center alteration to information by guaranteeing that the information landing at the collector, the hub is in unaltered structure and stays as transmitted by the sender.

Vermesan and Friess [7] discussed security and privacy framework requirements in dealing with IoT security challenges, as follows:

Authentication and Authorization

Authentication and authorization are crucial security requirements for IoT. These mechanisms ensure that only authorized users can access IoT devices and data. Authentication verifies the identity of users, while

authorization ensures that they have the necessary permissions to access the data. Authentication and authorization can be implemented using techniques such as usernames and passwords, biometric authentication, and multi-factor authentication.

Data Encryption

Data encryption is another vital security requirement for IoT. It ensures that data transmitted and stored by IoT devices is protected from unauthorized access. Encryption converts plain text into cipher text, making it unreadable without the decryption key. Data encryption can be implemented using encryption algorithms such as Advanced Encryption Standard (AES) and RSA.

Secure Communication

Secure communication is essential to ensure that data transmitted between IoT devices and other systems is protected from interception and tampering. Secure communication can be implemented using protocols such as Transport Layer Security (TLS), Secure Sockets Layer (SSL), and Virtual Private Network (VPN).

Secure Firmware Updates

IoT devices require firmware updates to fix bugs and security vulnerabilities. Secure firmware updates ensure that the updates are genuine and not malicious. Secure firmware updates can be implemented using techniques such as code signing and secure boot.

Secure Storage

IoT devices store sensitive data such as user credentials, personal information, and device configurations. Secure storage ensures that this data is protected from unauthorized access. Secure storage can be implemented using techniques such as data encryption, access control, and tamper detection.

Device Management

Device management is critical to ensure the security of IoT devices. It involves activities such as device registration, device configuration, and device monitoring. Device management ensures that only authorized devices are connected to the network and that devices are configured with the necessary security settings.

Physical Security

Physical security is essential to protect IoT devices from theft and tampering. Physical security involves measures such as securing devices with locks and alarms, monitoring access to devices, and ensuring that devices are stored in secure locations.

- Lightweight and symmetric solutions to support resource constrained devices.
- Lightweight key management systems to enable the establishment of trust relationships and distribution of encryption materials using minimum communication and processing resources, consistent with the resource constrained nature of many IoT devices.
- Cryptographic techniques that enable protected data to be stored processed and shared, without the information content being accessible to other parties.

- Techniques to support (" Privacy by Design") concepts, including data identification, authentication and anonymity.
- Keeping information as local as possible using decentralized computing and key management. • Prevention of location privacy and personal information inference that individuals may wish to keep private by observing IoT-related exchanges.

VI. CONCLUSION

The fundamental objective of this paper was to give an important study of the most significant parts of IoT with specific concentrate on the vision and security challenges associated with the Internet of Things. The vision of IoT will permit individuals and things to be associated whenever, anyplace, with anything furthermore, anybody, in a perfect world utilizing any way organize and any administrations. IoT target creating smart environment autonomous devices. Smart city transports smart schools for student tracking study. Challenges facing in security and privacy in IoT.

VII. REFERENCES

[1]. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," Future Generation Computer Systems, 2013.

[2]. L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787–2805, Oct. 2010. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2010.05.010

[3]. D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization," Wireless Personal Communications, vol. 58, no. 1, pp. 49–69, 2011.

[4]. 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.

[5]. D. Yang, F. Liu, and Y. Liang, "A survey of the internet of things," ICEBI-10, Advances in Intillegant Systems Research, ISBN, vol. 978, pp. 90–78 677, 2010.

[6]. H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelffle, "Vision and ´ challenges for realising the internet of things," Cluster of European Research Projects on the Internet of Things, European Commision, 2010.

[7]. O. Vermesan and P. Friess, Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems. River Publishers, 2013.

[8]. O. Mazhelis, H. Warma, S. Leminen, P. Ahokangas, P. Pussinen, M. Rajahonka, R. Siuruainen, H. Okkonen, A. Shveykovskiy, and J. Myllykoski, "Internet-of-things market, value networks, and business models : State of the art report," 2013.

[9]. M. Covington and R. Carskadden, "Threat implications of the internet of things," in Cyber Conflict (CyCon), 2013 5th International Conference on, 2013, pp. 1–12.

[10]. R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," Computer, vol. 44, no. 9, pp. 51–58, 2011.

[11]. H. Suo, J. Wan, C. Zou, and J. Liu, “Security in the tnternet of things: A review,” in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, vol. 3. IEEE, 2012, pp. 648–651.

[12]. G. Yang, J. Xu, W. Chen, Z.-H. Qi, and H.-Y. Wang, “Security characteristic and technology in the internet of things,” Nanjing Youdian Daxue Xuebao(Ziran Kexue Ban)/ Journal of Nanjing University of Posts and Telecommunications(Natural Nanjing University of Posts and Telecommunications(Natural, vol. 30, no. 4, 2010.

[13]. M. Abomhara and G. M. Køien, “Security and privacy in the internet of things: Current status and open issues,” in Privacy and Security in Mobile Systems (PRISMS), International Conference on. IEEE, 2014, pp. 1–8.

[14]. A. de Saint-Exupery, “Internet of things, strategic research roadmap,” 2009

[15]. A. u. Rehman, S. U. Rehman, I. U. Khan, M. Moiz and S. Hasan, "Security and Privacy Issues in IoT," International Journal of Communication Networks and Information Security (IJCNIS), vol. 8, no. 3, pp. 147-157, 2016.

[16]. R. Khan, S. U. Khan, R. Zaheer and S. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," in 2012 10th International Conference on Frontiers of Information Technology (FIT):, 2012.

[17]. A. Mahendra, "Biggest Challenges For The Internet of Things (IoT)," 21 06 2015. [Online]. Available: http://iotworm.com/biggest-challenges-for-theinternet-of-things.

[18]. J. Lopez, R. Roman, and C. Alcaraz, “Analysis of security threats, requirements, technologies and standards in wireless sensor networks,” in Foundations of Security Analysis and Design V. Springer, 2009, pp. 289–338.