IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 7, June 2022
Impact Factor: 6.252

# Survey on IOT Security and Privacy

**Prof. Nilam Ajay Jadhav[1], Prof. Gayatri Shrikant Mujumdar[2], Prof. Bhagyashali Vikram Jadhav[3]**
Lecturer, Department of Computer Engineering[1,2,3]
Pimpri Chinchwad Polytechnic College, Pune, Maharashtra, India

**Abstract:** *This paper introduces Internet of Things (IoTs), which offers capabilities to identify and connect worldwide physical objects into a unified system. As a part of IoTs, serious concerns are raised over access of personal information pertaining to device and individual privacy. This survey summarizes the security threats and privacy concerns of IoT. This survey also tell us about the applications of IOT and what are the network system used in IOT and the intelligent system used in IOT.*

**Keywords:** Internet of IOT Threats, Security, Privacy.

## I. INTRODUCTION

With the rapid development of Internet technology and communications technology, our lives are gradually led into an imaginary space of virtual world. People can chat, work, shopping, keeps pets and plants in the virtual world provided by the network. However, human beings live in a real world, human activities cannot be fully implemented through the services in the imaginary space. It is the limitation of imaginary space that restricts the development of Internet to provide better services. To remove these constraints, a new technology is required to integrate imaginary space and real-world on a same platform which is called as Internet of Things (IoTs). Based on a large number of low-cost sensors and wireless communication, the sensor network technology puts forward new demands to the Internet technology. It will bring huge changes to the future society, change our way of life and business models.

Apart from benefits of IoTs, there are several security and privacy concerns at different layers viz; *Front end, Back end and Network*. In this paper, the survey is in several security and privacy concerns related to Internet of Things (IoTs) by defining some open challenges. Then, discussion on some applications of IoTs in real world.

Rest of the paper is organized as follows: Section 2 gives an overview, background and real life applications of IoTs. Security and privacy concerns in IoTs are discussed in Section
3. Section 4 concludes survey study with references at the end.

### 1.1 What is the Internet of Things?

As shown in Fig. 1, the IoTs allow people and things to be connected anytime, anyplace, with anything and anyone, ideally using any path/network and any service [1]. They are "Material objects connected to material objects in the Internet".

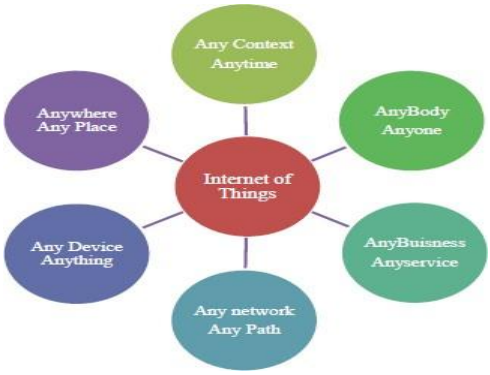


Fig 1.Defination of IOT

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 7, June 2022
Impact Factor: 6.252

For example, through RFID, laser scanners, global writing system, infrared sensors and other information sensing devices are connected to any object for communication services and data exchange. At last, to reach the smart devices to be tracked, located, and monitored and to handle the network functions, to make the IT infrastructure and physical infrastructure consolidation IoT is the most needed one.

## II. EVOLUTION

Before the investigation of the IoTs in depth, it is worthwhile to look at the evolution of the Internet. As shown in Fig. 2, in the late 1960s, communication between two computers was made possible through a computer network. In the early 1980s, the TCP/IP stack was introduced. Then, commercial use of the Internet started in the late 1980s. Later, the World Wide Web (WWW) became available in 1991 which made the Internet more popular and stimulate the rapid growth. Then, mobile devices connected to the Internet and formed the mobile- Internet. With the emergence of social networking, users started to become connected together over the Internet. The next step in the IoTs is where objects around us will be able to connect to each other (e.g. machine to machine) and communicate via internet.

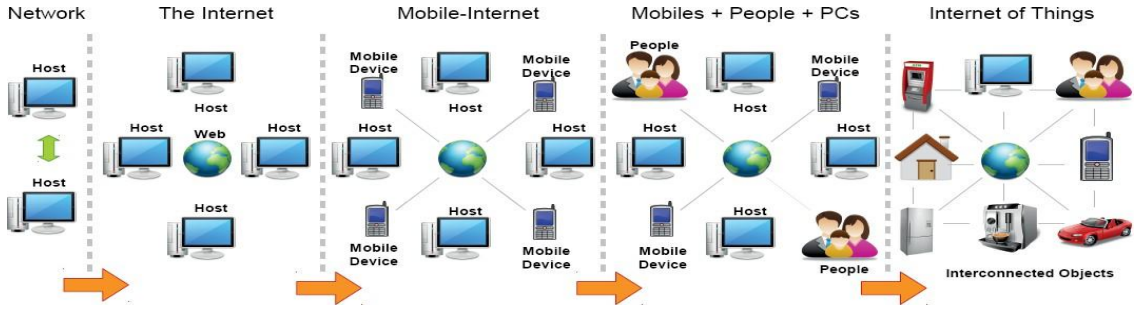


Fig 2. Evolution of Internet

## III. ARCHITECTURE AND PROTOCOL STACK OF IOTS

IoTs can be divided into three important layers Viz; Perception, Network and Application. As shown in Fig.3, perception layer (also called as recognition layer) gathers data/information and identifies the physical world. Network layer is the middle one (also called as wireless sensor networks), which accountable for the initial processing of data, broadcasting of data, assortment and polymerization. The topmost application layer offers these overhauls for all industries. Among these layers, the middle one network layer is also a "Central Nervous System" that takes care of global services in the IoTs, since it acts the part of aggregating with upward application layer and makes the link downward of perceptual layer.

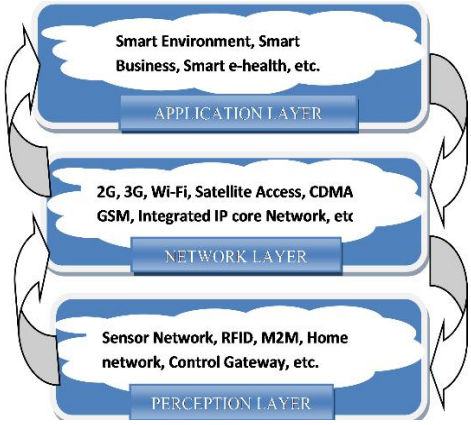


Fig 3 Architecture of IOT

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 7, June 2022
Impact Factor: 6.252

### 3.1 IOT Protocol Stack

From a networking perspective, the introduction of the IETF 6LoWPAN protocol family has been instrumental in connectingthe low power radios to the Internet and the work of IETF ROLL allowed suitable routing protocols to achieve universal connectivity. From the transport layer and an application perspective, the introduction of the IETF CoAP protocol family has been instrumental in ensuring that application layers and applications themselves do not need to be re-engineered to run over low-power embedded networks .

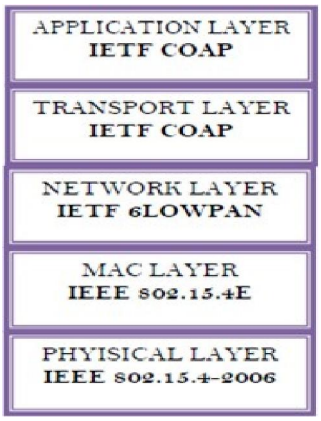


Fig 4.IoT Protocol stack

## IV. APPLICATIONS OF IOT

A survey done by the IoT-I project in 2010 [4]identified IoTs application scenarios which are grouped in 14 domains viz; Transportation, Smart Home, Smart City, Lifestyle, Retail, Agriculture, Smart Factory, Supply chain, Emergency, Health care, User interaction, Culture and tourism, Environment and Energy.

### 4.1 IoTs in Medical Application

Due to population growth, rural urbanization, declining birthrate, population aging, economic growth and social unbalanced resource utilization, some social problems have become increasingly apparent in the healthcare field.

- The health management level and the incapability ofresponding to emergency is a pressing social problem.
- There is a serious shortage in medical staffs, institutional facilities especially in rural areas, lack of medical facilities, lowlevel of treatment, inadequate healthcare system
- The imperfect diseases prevention system cannot meet the national strategy requirements to safeguard the health of the citizen becoming heavy burden on economy, individuals, families and state.
- Inadequate disease prevention and early detection capability.

To address these issues, Remote Monitoring and Management Platform of Healthcare information (RMMP-HI) [5] can provide monitoring and management of these lifestyle diseases so as to reach the purpose of prevention and early detection.

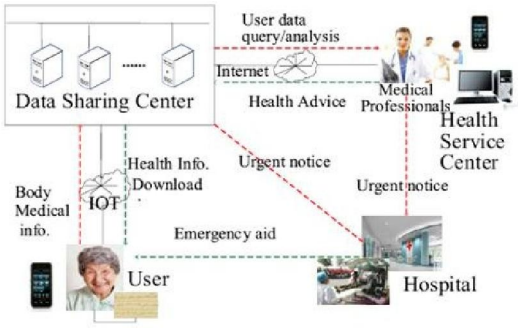


**Fig 5** The framework of healthcare service

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 7, June 2022
Impact Factor: 6.252

### 4.2 IoT in Smart Home

Now a days, smart homes are becoming more and more cost- effective and intellectualized with continued progress and cost reduction in communication technology, information technology, and electronics, which connects the Internet with everyday devices and sensors for connecting virtual and physical objects through the data capture and communication capabilities development.


Fig 6 IOT in Smart Home

In addition, by virtue of smart home systems, windows, home ventilation, doors, lighting, air conditioningetc., can be controlled by remotely. Each electronics devices such as refrigerator, washing machine, oven etc., can be manipulated by remote platforms or programs. Entertainment equipment's like radios and televisions can be connected to common channels which are in remote. In addition, home security and healthcare are also important aspects of smart homes. For instance, health aid devices can help an elder individual to send request or alarm to a family member or a professional medical center.

## V. SECURITY AND PRIVACY CONCERNSIN IOT

### 5.1 Security Concerns in IoTs

Internet of Things virtually is a network of real world systems with real-time interactions. The development of the initial stage of IoT, is M2M (Machine to Machine), having uniquecharacteristics, deployment contexts and subscription.Unattended operation without human intervention is possiblefor long periods of time by the wireless area network (WAN) or WLAN.

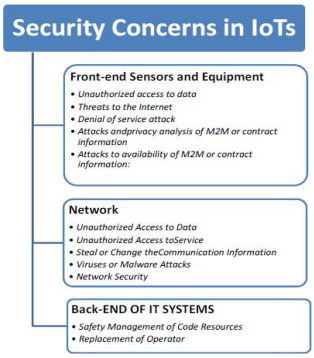


Fig 7 Security Threats in IOT

Network plays an important role providing a more comprehensive interconnection capability, effectualness and thriftiness of connection, as well as authentic quality of service in IoTs. Back-end IT systems form the gateway, middleware, which has high security requirements, and gathering, examining sensor data in real time or pseudo real-time to increase business intelligence.

### 5.2 Privacy Concerns in IOT

The Internet security glossary [9] defines privacy as "the rightof an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with itsenvironment, including the degree to which the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 7, June 2022
Impact Factor: 6.252

entity is willing to share information about itself with others". Privacy should be protected in the device, in storage during communication and at processing which helps to disclose the sensitive information.

### 5.3 Privacy in Device

The sensitive information may be leaked out in case of unauthorized manipulation or handling of hardware and software in these devices. For example, an intruder can "re- programme" a surveillance camera could such that it sends data not only to the legitimate server, but also to the intruder. Thus, for devices that gather sensitive data robustness and tamper- resistance are especially important.

### 5.4 Privacy during Communication

To assure data confidentiality during the transmission of the data, the most common approach is encryption. Encryption on certain occasions adds data to packets which provides a way fortracing, e.g. sequence number, IPsec- SecurityParameterIndex, etc. These data may be victimized for linking packets to the analysis of same flow traffic.

### 5.5 Privacy in Storage

For protecting privacy of information storage, followingprincipals should be considered.

- Only the least possible amount of information should bestored that is needed.
- In case of mandatory then only personal information retained.
- Information is brought out on the basis of "need-to-know".

### 5.6 Privacy at Processing

It is mainly of two folds. Firstly, personal data must be treated in a way that it should be simpatico with the intended purpose. Secondly, without explicit acceptance and the knowledge of the data owner, their personal data should not be disclosed or retained to third parties. By considering the above two points, Digital Rights Management (DRM) systems [15] is most suitable which controls the consumption of commercial media and defendsagainst re-distribution illegally.

## VI. CONCLUSION

The IoT technology draws huge changes in everyone's everyday life. In the IoTs era, the short-range mobile transceivers will be implanted in variety of daily requirements. The connections between people and communications of peoplewill grow and between objects to objects at anytime, in any location. The efficiency of information management andcommunications will arise to a new high level. The dynamic environment of IoTs introduces unseen opportunities for communication, which are going to change the perception of computing and networking. The privacy and security implications of such an evolution should be carefully considered to the promising technology. The protection of data and privacy of users has been identified as one of the key challenges in the IoT.

## REFERENCES

**[1].** S. M. Metev and V. P. Veiko, Laser Assisted Microtechnology, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

**[2].** J. Breckling, Ed., The Analysis of Directional Time Series: Applications to Wind Speed and Direction, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.

**[3].** S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," IEEE Electron Device Lett., vol. 20, pp. 569–571, Nov. 1999.

**[4].** M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in Proc. ECOC'00, 2000, paper 11.3.4, p. 109.

**[5].** R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, "High-speed digital-to-RF converter," U.S. Patent 5 668 842, Sept. 16, 1997.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 7, June 2022
Impact Factor: 6.252

**[6].** (2002) The IEEE website. [Online]. Available: http://www.ieee.org/

**[7].** M. Shell. (2002) IEEEtran homepage on CTAN. [Online]. Available: http://www.ctan.org/tex-archive/macros/latex/ contrib. /supported/ IEEEtran/

**[8].** FLEXChip Signal Processor (MC68175/D), Motorola, 1996.

**[9].** "PDCA12-70 data sheet," Opto Speed SA, Mezzovico, Switzerland.

**[10].** A. Karnik, "Performance of TCP congestion control with rate feedback: TCP/ABR and rate adaptive TCP/IP," M. Eng. thesis, Indian Institute of Science, Bangalore, India, Jan. 1999.

**[11].** J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control," Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.

**[12].** Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997