A Survey on Internet of Things: Security and Privacy Issues

MADHURA P M
6th Semester B.E.
ISE SJB Institute of Technology
Bangalore Karnataka, India

NAMRATA BILURKAR
6th Semester B.E.
ISE SJB Institute of Technology
Bangalore Karnataka, India

PALASH JAIN
6th Semester B.E.
ISE SJB Institute of Technology
Bangalore Karnataka, India

RANJITH J
Asst.Professor
Dept. of ISE
SJBIT Bangalore Karnataka, 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.

I. INTRODUCTION

With the rapid development of Internet technology our lives are gradually led into an imaginary space of virtual world. People can chat, work, shop , keep pets and plants in the virtual world provided by the network. However, 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 on the Internet technology.

Apart from benefits of IoTs, there are several security and privacy concerns at different layers; Front end, back end and Network. This paper surveys the several security and privacy concerns related to Internet of Things (IoTs) by defining some open challenges, and discusses some applications of IoTs in real world.

II. IOT OVERVIEW AND BACKGROUND

2.1. What is the Internet of Things?

The IoTs allow people and things to be connected anytime, anyplace, with anything and anyone, ideally using any path/network and any service. They are “Material objects connected to material objects in the Internet”.

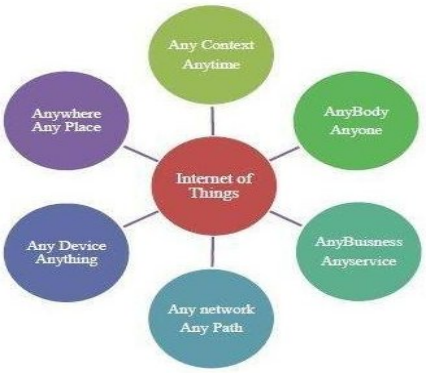

Fig. 1 Definition of Internet of Things.

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.

2.2. Evolution

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 the Internet.

IoT promises to create a world where all the objects (also called smart objects) around us are connected to the Internet and communicate with each other with minimum human intervention. The ultimate goal is to create "a better world for Human beings" where objects around us know what we like, what we want, and what we need and act accordingly without explicit instructions.

2.3. Architecture and Protocol Stack of IoTs

IoTs can be divided into three important layers Viz; Perception, Network and Application. 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.

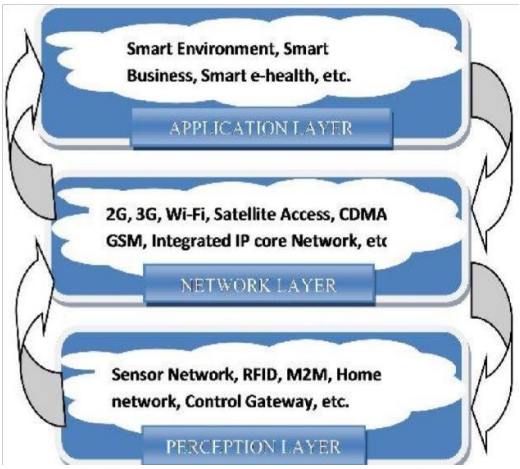

Fig.2.a. Architecture of Internet of things.

Various basic networks including, mobile/ private network, wireless and wired network offers and affirms the underlying connection. IoTs are set up in this new network which is composed Business applications of networks.

Regarding the IOT Protocol Stack, from a PHY perspective, the current IEEE 802.15.4-2006 PHY layer(s) suffice in terms of energy efficiency. Given that a large amount of IoT applications however will require only a few bits to be send. It may be advisable to commence looking into a standardized PHY layer which allows ultra-low rate transmissions over very narrow frequency bands, with the obvious advantage of enormous link budgets and thus significantly enhanced ranges. IEEE802.15.4e standard is very suitable for a protocol stack for IoT because it is latest generation of highly reliable and low-power **MAC** protocol.

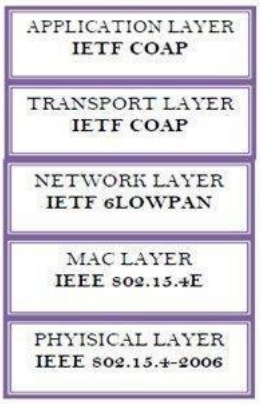

Fig 2.b. IOT Protocol Stack.

From a networking perspective, the introduction of the IETF 6LoWPAN protocol family has been instrumental in connecting the low power radios to the Internet and the work of IETF ROLL allowed suitable routing protocols to achieve universal connectivity.

2.4. Applications of IOTs

A survey done by the IoT-I project in 2010 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.

2.4.1. 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.

Remote Monitoring and Management Platform of Healthcare Information (RMMP-HI) can provide monitoring and management of lifestyle diseases so as to reach the purpose of prevention and early detection.

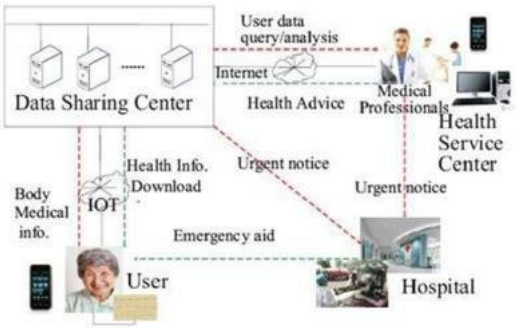

Fig.3. The framework of Healthcare service

Regardless of restrictions of location, time, and user' activity state, RMMP-HI can collect human body medical information timely through a variety of body medical sensors loaded in the human body or

surrounding space and extract useful information by data encryption, storage, comparative analysis and processing. When abnormal appearance is found, users are notified to take early treatment; this enables the early detection and prevention. Furthermore, it is also efficient to establish national health management records, to provide prevention and decision- making basis for lifestyle diseases, epidemic and regional disease through monitoring, comparing analyzing and processing healthcare information of associated group. In this way, capabilities of disease prevention, early detection and early treatment are improved enormously.

Body medical sensors can register and delete, constituting Medical Body Area Network (MBAN) automatically. Short-range wireless communication sensor module will transmit human medical information to 3G mobile phone or home gateway. This medical information is uploaded to data storage and processing center timely. Then the important health guidance will be fed back to the patient, family members of patients or medical institutions after analytical processing of expert system or the inspection of professional medical staff in health service center. In the state of emergency, first-aid notification is delivered to medical institution by health service center to provide emergency services to patients.

2.4.2. 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.4. IoT Smart Home.

By virtue of smart home systems, windows, home ventilation, doors, lighting, air-conditioning etc. can be remotely controlled. Each electronic device can be manipulated by remote platforms. Entertainment equipment 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.

2.4.3. Intelligent community security system (ICSS)

The intelligent community security system (ICSS) holds several subsystems, such as Vehicle Management Subsystem (VMS), Surrounding Security Subsystem (SSS), Central Information Processing System (CIPS), Property Management Subsystem (PMS), Fire and Theft Prevention Subsystem (FTPS) etc.

Through wireless the information of each subsystem is messaged to the CIPS implies automatic adjustments and timely warnings in order to maintain the community security. The details about ICSS subsystems are as follows:

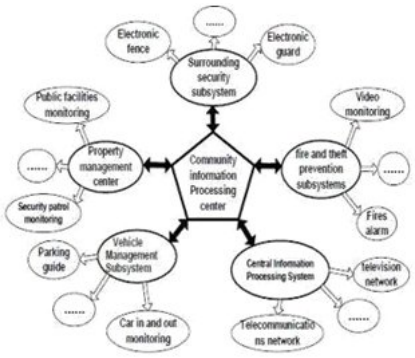

Fig.5. intelligent Community Security System (ICSS).

2.4.3.1. Vehicle Management Subsystem of the ICSS

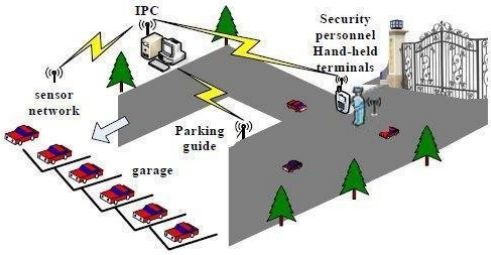

Fig. 6. Vehicle Management Subsystem.

The Vehicle Management Subsystem in ICSS adopts IPR, sensor network technologies and RFID. Image registration can be taken by RFID card and video camera which is given to the vehicles. The vehicle license information will be messaged to the CIPS, when it enters the communities. The visitors are allocated with the temporary parking places. The record data and the information of the driver' RFID card must be coherent, when the car leaves. This guarantees the security of cars and prevents theft occurrences. In the garages video monitoring devices will prevent stealing or damage to assure the vehicles safety. Through the Human-Computer interface system CIPS can controls the garages to facilitate and

observe the vehicle management.

2.4.3.2. Surrounding Security Subsystem (SSS)

As per the requisites of security surroundings to establish an intelligent and enclosed community, sensing terminals such as Power Network, Unicode Infrared Laser and Sensor Optical Fi ber etc. are installed

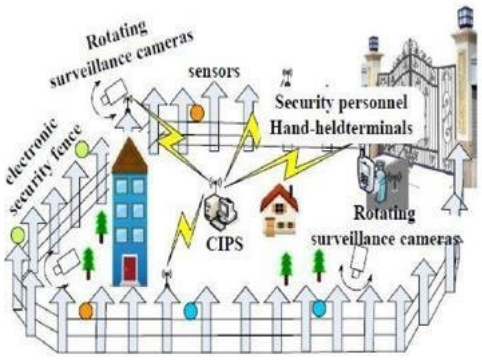

Fig.7. Surrounding Security Subsystem.

The SSS contains electronic access controls, electronic fences and rotatable monitoring cameras. It can be utilized to avoid illegal enter or intrusive behavior into communities. The subsystem can find the exact location of the accident by using sensing terminals which can automatically omit untrue signals. The rotatable cameras will track the people or objects by IPR technology; simultaneously they triggers alarm to the handheld devices of the security personnel and CIPS through the sensor network.

2.4.3.4. Fire and Theft Prevention Subsystem (FTPS)

Electrical equipment's and appliances may induce huge potential dangers. The FTPS can be used for the indoor security. It contains anti-theft and anti-fire alarm system, video monitors and emergency alarm functions, etc. The system primarily use the uniform coded of sensing window fences, monitor cameras, entrance guard devices, emergency calling devices , temperature sensors, and smart detectors of smoker combustible gas. To form the network of this subsystem home network, sensor network and the CIPS were used.

III. SECURITY AND PRIVACY CONCERNS IN IOTS

3.1. 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 unique characteristics, deployment contexts and subscription. Unattended operation without human intervention is possible for long periods of time by the wireless area network (WAN) or WLAN. In spite of being socially efficient, it creates an array of new problems concerning breach of privacy and information security.

3.1.1. Front-End sensors and equipment

Front-end sensor and equipment receiver's data via the built in sensors. They then don't transmit the data using modules or M2M device, thus achieving networking services of multiple sensors, the methodology involves the security of machine with business implementation and node connectivity

Machine or perception node are mostly distribution in the absence of monitoring scenarios. An intruder can easily access these device which imply damage or illegal action on these node can be done. Possible threads are analyzed and categories to unauthorized access of data. Threads to internet and denial of service attacks

3.1.2. Network

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. Since a large number of machines sending data to network congestion, large number of nodes and groups exist in IoTs may be resulted in denial of service attacks.

3.1.3. Back-end of it systems

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. The security of IoT system has seven major standards viz; privacy protection, access control, user authentication, communication layer security, data integrity, data confidentiality and availability at any time.

3.2. Privacy Concerns in IOTs

The Internet security glossary defines privacy as "the right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others".

Typically in IoTs, the environment is sensed by connected devices. They then broadcast the gathered information and particular events to the server which carries out the application logic. This is performed by Mobile or/and fixed communication which takes the responsibility.

Privacy should be protected in the device, in storage during communication and at processing which helps to disclose the sensitive information privacy of users and their data protection have been identified as one of the important challenges which need to be addressed in the IoTs.

3.2.1. 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- program" 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. To ensure IoTs security trusted computing technologies including device integrity validations, tamper-resistant modules and trusted execution environments are useful.

In order to provide the privacy in the devices, there exists so many problems one need to address, it could be the location privacy of the device holder, non-identifiability means protecting the identification of the exact nature of the device, protecting the personal information in case of the device theft or loss and resilience to side channel attacks. Location Privacy in WSN is achieved by using the algorithm Multi-Routing Random walk in the wireless sensors, in the case of the Protecting of display privacy and Protection of personal Identifiable Information (PII) in case of device loss, theft could be achieved by using QR codes (Quick Response Code) Technique. In the case of Non-Identifiability and side Channel attacks adding randomness or noise, having synchronous CPUs, blind values used in calculations could be used.

3.2.2. 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 for tracing, e.g. sequence number, IPsec- Security Parameter Index, etc. These data may be victimized for linking packets to the analysis of same flow traffic. Secure Communication Protocol could be the suitable approach.

During the communication Pseudonyms can be replaced for encryption in case it is not feasible to the device's identity or user's in order to decrease the vulnerability. One of the long-familiar examples is Temporary Mobile Subscriber Identity (TMSI). Devices should communicate if and only if when there is a need, to derogate privacy disclosure induced by communication.

3.2.3. Privacy in Storage

For protecting privacy of information storage, following principals should be considered.

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

To conceal the real identity tied with the stored data Pseudonymization and Anonymization could be used. Without disclosing any specific record, a database could allow access only To statistical data (sum, average, count, etc.). To ensure the output (typically aggregate queries) is independent of the absence or presence of a particular record adds noise called as differential privacy could be the appropriate technique.

3.2.4. 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.

In consideration of above points, Digital Rights Management (DRM) systems is most suitable which controls the consumption of commercial media and defends against re-distribution illegally. One can define privacy policies for personal data in a rights object or license instead of exercising principles for commercial media which must be obeyed during the data processing. DRM requires trusted devices, secure devices to work efficiently and effectively. sers' permission and their awareness are requirements for distribution of personal data. User notification aids to avoid abuse.

IV. 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 people will grow and between objects to objects at any time, in any location. The efficiency of information management and communications will arise to a new high level. The privacy and security implications of such an evolution should be carefully considered by the promising technology. The protection of data and privacy of users has been identified as one of the key challenges in the IoT.

In this survey, we presented Internet of Things with architecture and design goals. We surveyed security and privacy concerns at different layers in IoTs. In addition, we identified several open issues related to the security and privacy that need to be addressed by research community to make a secure and trusted platform for the delivery of future Internet of Things. We also discussed applications of IoTs in real life. In future, research on the IoTs will remain a hot issue.

V. ACKNOWLEDGEMENTS

The authors thank Dr.S.Sridhar, Professor and Dean, Cognitive & Central Computing Facility of R.V.College of Engineering, Bangalore, India for communicating this paper to this Journal for publication.

VI. REFERENCES

[1] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context Aware Computing for The Internet of Things: A Survey" IEEE Communications Surveys & Tutorials, 2013, pp. 1-41

[2] G. Gang, L. Zeyong, and J. Jun, "Internet of Things Security Analysis," 2011 International Conference on Internet Technology and Applications (iTAP), 2011, pp. 1-4.

[3] M. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia, and M. Dohler, "Standardized protocol stack for the internet of (important) things," Proceedings of IEEE, 2012, pp. 1-18.

[4] O. Vermesan, P. Friess, and A. Furness, The Internet of Things 2012, By New Horizons, 2012. [Online]. state-of-the-art survey," International Conference on Communication Systems (ICCS),Proceedings of IEEE, Available: http://www.internet-of-things-research.eu/pdf/IERC_Cluster_ Book_2012_WEB.pdf

[5] W. Zhao, C. Wang, and Y. Nakahira, "Medical Application on IoT," International Conference on Computer theory and Applications, 2011, pp. 660-665.

[6] K. Bing, L. Fu, Y. Zhuo, and L. Yanlei, "Design of an Internet of things-based Smart Home System," 2nd International Conference on Intelligent Control and Information Processing, 2011, pp.921-924.

[7] D. Jiang, C. Shiwei, "A Study of Information Security for M2M of IoT," 33rd International Conference on Advanced Computer Theory and Engineering, 2010, pp. 576-579.

[8] RFC 2828, "Internet Security Glossary," May 2000, [Online]. Available: https://www.ietf.org/rfc/rfc2828.txt.

[9] R. Hall, A. Rinaldo and L. Wasserman, "Differential Privacy for Functions and Functional Data," Journal of Machine Learning Research, 2013, pp.703-727.

[10] E. Liu, Z. Liu and F. Shao, "Digital Rights Management and Access Control in Multimedia Social Networks" in Genetic and Evolutionary Computing, Springer International Publishing, 2014, pp.257-266.

