RESEARCH ARTICLE   OPEN ACCESS

A STUDY ON SECUIRTY ASPECT OF IOT

Akshay Dakare[1], Megha Bramhankar[2], Prof. Suyog Gupta[3]

1(Department of Electronics and Telecommunication Engineering, *S.R.P.C.E, Nagpur.*Email: ad2u9484@gmail.com)
2(Department of Electronics and Telecommunication Engineering, *S.R.P.C.E, Nagpur.*Email: megha.bramhankar@gmail.com)
*3(Department of Electronics and Telecommunication Engineering, S.R.P.C.E, Nagpur.*Email: suyog@ srpce.ac.in)

Abstract:

The internet of things (IOT) is most important technology of future for connecting millions of devices. With technology evolving at rapid rate, our lives have 8/been integrated with them. Nations have taken a step into a new age of smart cities enabling technology to increase the quality of life. The Expansion in wireless communication is expected to generate large amount of data hence we must require strong secure system to protect that information. This project deals with study of Internet of Things (IOT).

Keywords — **IOT, Secure IOT, Security, Encryption.**

I. INTRODUCTION

InternetofThings, Bill Gates mentioned in "The Road Ahead" in 1995[1].Then in 2005, ITU published Internet. Report forecast its establishing will bring 1 billion the order of the information equipment, the order of 3.0 billion intelligent electronic devices, 500 billion off the micro - processor, the sensor needs more than trillion. Truly, Internet of Things is a huge boost engine in the future information industry, is the third bid wave of the information industry in computer network.

The Internet of Things is tool through which RFID, infrared sensors, global writing system, laser scanners and other information sensing equipment, connecting any object with Internet for information exchange and communication services. Ultimately, to achieve intelligent devices located, tracked, monitored and manage the functions of a network, to make the physical infrastructure and IT infrastructure unification.

Internet of Things isMaterial objects in the Internet connected with material object." There has two meanings can be explained: in the first place, the Internet is not only the core and foundation, but also based on and extension of the Internet. Another place, Client's extension and expansion make links between every things and any objects, generate information communication.

II. STRUCTURE

The biggest challenges faced when planning Internet of Things (IOT) solution is dealing with complexity.A typical IOT solution involves heterogeneous IOT devices, with sensors that produced data is then analysed to gain insights.

IOT devices are connected either directly to a network or through gateway devices to communicate with each other and with cloud services and applications.

Edge computing describes the work that happens at the edge of the IOT network, where the physical devices connect to the cloud. With focus on reducing latency, improving privacy and reducing bandwidth. Costs within data driven IOT applications, edge computing architecture are becoming more common within IOT.
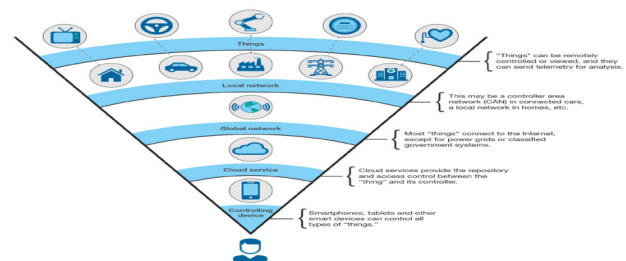

Figure 1. Internet of things structure figure

III. SECURITY REQUIREMENTS

Network layer, has various properties. Needs security of sensor stock, operation and sending information and inhibit unauthorized accessing even notlegal process, called ulterior. Asked to each node which participate in information processing is authentic reliable, call authenticity. Requests transmission of information has not been destroyed without authorization, with along integrity. Request every gateway working and provide best services, as availability. The sending and receiving data must be latest and updated, not the attacker modifying, definition as Data Fresh. In addition, with the characteristics of low-cost, disposable, unattended, sensors are easy damaged, broken up and physical access even controlled. Therefore, scalability require for wireless sensor network. Or in such circumstances like some nodes working abnormal, adding new nodes and adjust nodes, like maintaining a large number error-prone and easily controlled sensors' network that requires infinite self-organization and automatically network. Then, the properties of network that have relationship shown.
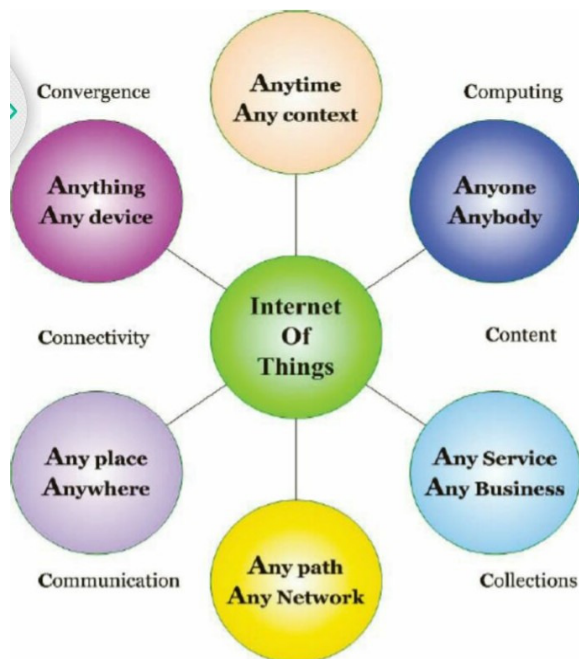in Figure 2:

Figure 2. Internet of things structure figure

IV. PAY ATTENTION TO THE SAFETY

The relationship between Internet of Things and Internet is inseparable and complementary. However, not the same in the form of network organization and in network functionality andin performance requirements of the two networks. Internet--based on the priority management typical characteristic make it not very require safe, reliable, controllable and manageable. But, Internet of Things heavily dependent on some aspects including real-time, safe and reliable, resource assurance. Along with Internet of Things brings new technologies rising, Information security escape from periods which are traditional virus infections, hackers and misusing of resources,
Forward a complex and diverse, comprehensive interactive period. In addition, Internet of Things mainly consists of sensor network and M2M parts which can be seen as sensor module and network layer constitute a large network together.
One point should be taken seriously, massive levels of network terminals and signal source exposed in a public place, if the network transmission control system or software have problems, the consequences is very serious. Currently, Internet's development encounter two big system bottlenecks problems, one is the IPv4 address is not enough, the other is the network itself security [4]. Through
IPv6 resolve address deficiencies, however, there isn't a good solution for the current network security. In a word, network manageable, controlled and service quality issues are not deal well, to achieve accurate, efficient, real-time network signal Transmission is flanker in the air, and will affect the further development.

V. SECURITY ISSUES

Wireless sensor network's characteristics present new challenges in information security area. Along with one-time, unattended, wireless communications, low-cost and resource constrained , sensors easily appear to abnormalities, physical Attacks by attackers, Trojan attacks, virus damage, keys decryption, DOS, eavesdropping and traffic analysis are really threats. The trouble is a

challenge that design of key storage, distribution, encryption and decryption mechanism caused by
Wireless sensor networks large and resource constraints [5].In the traditional system, network layer security and application layer security is independent, just as communication between the leaderships and communication between the secretaries is different. Internet of Things is on
The basis of the existing mobile network platform integrate sensor networks and Internet that make large amount of special problem of it. This situation can be said combine with leadership and secretary. Therefore, most of the mobile network communication system can still be applied to Internet of Things and provide security as authentication encryption and mechanisms. However, according to the characteristics of
The network layer, we need to adjust the system and add functions. For example :1)sensor network gateway nodes out of control ,2)network 's DOS attacks to sensor network nodes,3) interference, tampering and destruction to the network signal, 4) the problems including identified large number of sensor nodes, identification, certification and control.

A. Encryption gateway node

Obtain the cipher text without the key cannot decipher the plaintext. Similarly, when the gateway node encrypted, capture a node is not equal to control the node, such a sensor node is hard to be controlled because attacks need master key
Of the node. In this way, integrate the key that is sensor network internal communication nodes and the key that is the remote information processing shared platform as an important keynote. Who want get the key is very difficult in this case, which get a gateway node has not shared key with sensornetwork, he cannot control gateway node and get all information through it .Then he cannot tamper with the sendinginformation, only prevent some or all information are sent, but it would be easily detected by the remote information platform. In this case, when an administrator found an abnormal sensor network, he will take some appropriate measures to reduce even avoid a great loss that caused by abnormal network sending false information.

B. Enhance the capacity againstDOS attack

Sensor network must connect with external networkeventually including the Internet, so they cannot escape attacks from other network. Currently, exclude the main attack illegal access, the other may be DOS attack. Since sensor network nodes resources which are computing and communications capabilities are limited, so the capacity against DOS attacks is weak. Therefore, sensor network nodes should have the ability to fight against DOSattacks, considered a direct access to the specific node inside net, such as remote control infrared system start-up and shutdown, ordinary nodes inside have less resources than gateway nodes ,so the capacity against DOS include both the gateway nodes and the ordinary nodes two types. Sensor networks connect with other network brings the problems which is not only it against external attacks, but also is how to authentication external device. So in the certification
Process, we must pay much attention to limited resources of sensor networks, then authentication mechanism we designed that the computational cost and communication cost must be as small as possible. In addition to the external Internet, theconnected with different sensor networks' number may be huge , how to distinguish between each network even nodes inside, how to identify them effectively, all of those are the premise to establish security mechanisms.

C. The encryption mechanism

The traditional network layer use by-hop encryptionMechanism that information in the transmission process needto keep decryption and encryption in each node make every node transmission in "clear text ", even encryption at the beginning of sending. And similarly, the traditional application layer encrypted end to end, which can be explained the "cleartext "in the sender and the receiver, each node is cipher text in the transmission time. As Internet of Things ' network layer and application layer connect closely, making us face using by- hop encryption or end to end encryption in the transmission. For by-hop encryption, it provides the protection to linkswhich asked necessary. Due to by-hop encryption in the

network layer so that we can apply to all business, which make different applications safety implement and management on the one network platform. In this way, security system is transparent to the business applications. By - Hop encryption ensure low latency, high efficiency, low cost and scalability characters. But, because the by-hopencryption requires decryption in the transmission nodes, so every node is likely to interpret the clear text message. In award: by-hop encryption demands high trustworthiness on the transmissionnodes. As for the end to end encryption, it can choose a different type business security policy, in order to provide high security protection for applications required high level security. However, end to end encryption cannot protect the destination address. Because each node through which a message should be as the destination address to determine how to transmit messages. This make end to end encryption not hide the message's source and destination, which is easy attacked by malicious access cause by analysis of the communication services. In addition to the perspective of national policy, end to end encryption cannot meet the national demand for the lawful interception policy. From these analysis, the security requirements of some business is not very high, under the environment that network can provide by - hop encryption protection, end to

end encryption is not very important in service layer requirement. But, to the high-security business, end to end encryption is still the first choice. Thus, due to the different requirements to the different security levels in business, wecan see end to end security in service layer as another option. As Internet of Things have started to accelerate develop, the security requirements of it is increasingly urgent, we need to figure out the special security requirements, then considerhow to provide end to end security protection. How to use existing mechanisms resolve these security features? The concept of the machine cluster is introduced by Internet of Things ' development, because of it, also need to outsider how to use machine group solving authentication problems.

Now days, Internet of Things is developing in the

Primary stage evens just a hot concept, not to talk about its implementation structure, etc. Thus, the safety mechanism of it is a blank in the industry, it is a long way for its research for and establish up.

D. Own unique problems

According to Internet of Things ' characteristics, it faces not only the traditional mobile communication network security issues but also some special security issues different fromexistent's. This is because it is constituted by a largeNumber of machines, lack of effective monitoring and management, which is large number equipment and cluster cause. These special problems mainly in the following areas. Internet of Things' machine--identify local node safety replace complex, dangerous and mechanical work, so the machine equipment are deployed in unattended outdoorscene, the attacker can easily access to these facilities and replace the parts of equipment and chip implanted Trojan horses, the consequences is unimaginable. These things will be designed and implemented well in the future, must set up early Warning systems and even automatic isolation.

The security issues of data transmission and information in sensor network. Sensor nodes usually have single functions temperature measurement and carry less energy, making

There have not complex monitoring and lacking of defence capacity. But ,the identity of the sensor network varieties form temperature measurement to hydrological monitoring, form road navigation to precise positioning, which have no specific criteria for the data transmission and the message

Signals. So we cannot provide a standardized security system, structure and the law.

The security issues of how to transfer data and signal in the core network. Core network with relatively complete protection and defence system, but, due to Internet of Tingshas large number of nodes and working in cluster,which maybe cause DOS service attacks by network congestion in

Transmission. Therefore, we must consider the load balancing algorithm for branch large amounts of data. In addition, the existing communication

network security architecture is for human not fit for physics objects communication, separating

The existing security mechanisms in machine - object and object - object logic relationship. Therefore, we must change the views in the implementation and the design process of it,To form a material-centre, human-traction scheme.

The issues of Internet of Things application security. As it may be first networked devices then connected to network, itis impossible to guard for the nodes in time, which is a bigtime-consuming problem how to sign remote configurationAnd business information. There will be a strong and unified security management platform for a large and diversenetwork. Otherwise, independent platform will be overwhelmed in all kinds of network applications. How to manage logs and information network become a new problem,How not to separate network and service platform trust relationship. These will be lead to new security problems.

VI. CONCLUSION

The Future of The World, must be intelligent virtual world, must be cloud computing and Internet of Things world. "With the technologies of it developing and deepen promoting. The three networks which are Internet of Things, The Internet and 3G mobile wireless networkswill continueapproach together. The more develop Internet ofThings, the more intelligent of it .While more areas of social has been widely application, the social will become information society in material to material and object to human.Meanwhile, we cannot ignore the security implications, because signal loss will directly affect the whole security of Internet of Things .Due to viruses, Trojan horses, hackers,

Malicious software are powerful and popular, which may restrict our travel and prevent us communications with others by invading our mobile phones. When virus running in our computers, we can stop and cut network to prevent the spread of virus. But what and how to do in this case, that virus spreadIn the network that the whole world become only one, are we prepared to deal with it? In fact, building Internet of Things is not only technical problems, but also involve in planning, infrastructure, management, security and other aspects problems.

References

1. *Zhao Hai-Xia. Internet of Things ' key technology Analysis and Discussion[J].Western Technology China,2010.4*

2. *Tan Xue-Qing, Fu Rui-Ping, Gao Qian. Identification is the Foundationof Internet of Things[J]. Automatic Identification Technology of China,2009.*

3. *Zhou Shuang-Yang. Find the High Place in Internet of Things[j].Communication World A,2009.*

4. *Bo Hong-Mei.Analysis Internet of Things 'technology[j].Technology Information Communication. 2010.*

5. *Zhao Zhang-Jie,Liu Hai-Feng. Wireless Sensor Network Security[J],Computer Security , 2010*

6. *Huang Hai-Kun, Deng Jia-Jia. Internet of Things Gateway Nodes,Technology and application [J].Telecommunication Science,2010*

7. *M. A. Simplicio Jr, M. V. Silva, R. C. Alves, and T. K. Shibata,"Lightweight and escrow-less authenticated key agreement for theinternet of things," Computer Communications, 2016.*

8. *L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey,"Computer networks, vol. 54, no. 15, pp. 2787–2805, 2010.*