INTERNET OF THINGS: SECURITY AND PRIVACY ISSUES

MOHD. SHAJID ANSARI[a1], SHANKEY GARG[b] AND SUBHASHINI SAHU[c]

[abc]RSR Rungta College of Engineering & Technology, Bhilai, Chhattisgarh, India

ABSTRACT

Rapidly growing technologies have become an essential part of modern life. But fact is, by using these technologies, it is easy to commit crimes. Thus, the security is important. The main focus is on the security issue of technology. A brief introduction of The Internet of Things which gives the lightweight solutions for resolving the security issues of transportation layer is well explained here. The three key security challenges for Internet of Things are also discussed here.

KEYWORDS: Internet-of-Things, Security issue, Challenges.

Recent advances in information, communication technologies and embedded systems have given rise to a new disruptive or rive technology: the Internet of Things (IoT)[5]. This major development will lead to major changes to a transformation of the technological ecosystem in all its complexity. The internet of Things (IoT) is the highly heterogeneous network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.

The Internet of Things (IoT) represents the interconnection of highly heterogeneous networked entities and networks following a number of communication patterns such as: thing-to-things (T2Ts) , thing-to-thing (T2T), human-to-thing (H2T) or human-to-human (H2H)[1]. The Internet of Thing (IoT) will help to allow an environment with the flexibility to provide services of all sorts, ranging from home automation to smart retail, and from smart environmental monitoring to smart city services. IoT is likely to improve the quality of people's lives, create new markets and new jobs, increase economic growth and be an stimulus for competition. However, IoT raises important Questions and introduces new challenges for the security of systems, processes and individuals. Some IoT applications are tightly linked to sensitive infrastructures and strategic services such as the distribution of water and electricity and the surveillance or guidance of assets[2]. Other applications require or manage sensitive information about people, such as their location and movements, or their health and purchasing preferences. Confidence in IoT will depend on the protection it gives or provides to people's privacy and the levels of security it guarantees to systems and processes.

IoT will allow objects to become active participants: these objects will be able to recognize events and changes in their environment and to sense and react autonomously without any human intervention. Introduction of objects into the control processes makes IoT security very difficult to address. Indeed, the Internet of things is a complex system where people interact with the technological ecosystem based on smart objects through complex processes. The four Iot components: persons, intelligent objects, technological ecosystem, and processes highlight a systemic and cognitive dimension to the security of IoT.

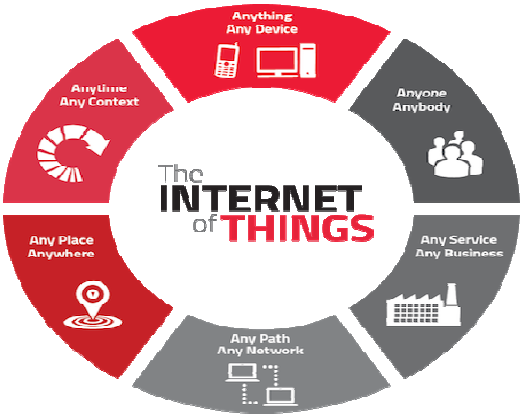

Figure 1: Internet of Things

The interaction of people with the technological ecosystem demands the protection of privacy of people. Similarly, their interaction with control processes demands to guaranteeing their safety.

OVERVIEW

Definition of (IoT)-

The internet of things (IoT) is a strategy of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer or exchange data over a network without requiring human-to human or human-to computer and without any human intervention .

"Things", in the IoT sense, can relate to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, automobiles with

built-in sensors and DNA analysis devices for environment.

Kevin Ashton, cofounder and executive director of Auto-ID Center at MIT, first introduced the term "Internet of Things" in a presentation he made to Procter and Gamble in 1999.

Comparison between IoT and tradition technology

IoT and traditional technology issues are different in many ways as follows-

The traditional Internet is a mature technology as it has standards in various areas and search engines that one can communicate with using natural languages. The net result is that the consumption of the traditional Internet can be done by everybody without the need of any technical skills. But in the IoT domain, the situation is little bit different. The standardization effort is required only in its first phases, thus, the data integration is done ad hoc and requires skilled programmers for implementing an application.

In the traditional Internet, the association is done through physical links between web pages. In the Internet of Things (IoT), the combination of or composite data is required for situation detection. This is cleared in the combining of data in the form of context-based event patterns in which some of the data determines the context and other determines the pattern itself.

Internet is framed of PC, smart phones whose resources are rich. So in the Internet, we can use fusions of complex algorithms and lightweight algorithms to maximize security with less considerations of resource usage such as computation power.

Topic	Traditional Internet	The Internet of Things (IoT)
Who creates content?	Human	Machine
How is the content consumed?	By request	By pushing information and triggering actions
How is the content combined?	Using explicitly defined links	Through explicitly defined operators
What is the value?	Answer questions	Action and timely information
What was done so far?	Both content creation (HTML) and content consumption (search engines)	Mainly content creation

Figure 2: Comparison between tradition internet & The Internet of Things

Similarly, there is also a difference in the value to the consumer. In the traditional Internet, the value resides in answering a question that is posed by the consumer, in most of the cases when searching for information or activating services. In the IoT, the value is timely or opportunely action or notification based on detected situations.

SECURITY CHALLENGES OF IOT

The Internet of Things (IoT) is the interconnecting physical devices, vehicle, buildings and other items. Actually, it can be implemented by using embedded with electronics devices, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data. There are mainly 3 challenges in the Internet of Things which are follows-

A Trillion Points Of Vulnerability

Every single device even sensor in the IoT represents a potential risk. Researchers at the French technology institute Eurecom downloaded some 32,000 firmware image from potential IoT device manufactures and found 38 vulnerabilities across 123 products including poor encryption and backdoors that could allow unauthorized access. And one weak link could open up access to hundreds of thousands of devices on a network which may cause serious consequences.

Trust And Data Integrity

Researchers have already proved that smart meters widely used in Spain, for example, can be hacked to under-report energy use. Unfortunately, they were able to spoof messages being sent from the meter to the utility company and send false data. Nowadays, we have been able to go to a high street store and buy anti-virus protection on a disc or download it straight to our PC. But in the IoT that security capability doesn't exist in most of the devices that will suddenly become connected.

Security must be built into the design of these devices to create trust in both the hardware and integrity of the data.

Data Collection, Protection And Privacy

All of the applications of IoT are to make our everyday lives easier and boost the efficiency and productivity of businesses and employees. The collected data will help us to make smarter decisions. But this will also have an impact on security & privacy expectations. If data collected by connected devices is compromised it will weaken trust in the IoT.

SECURITY ISSUES OF IOT AND THEIR SOLUTIONS

The transportation layer of IoT is also susceptible to Trojan horses, viruses, spam and other attacks resulting in information disclosure, network

paralysis, others such as middle attacks, replay attacks, access attacks, and phishing sites attacks and combo attacks. Although attacks are very common or familiar issues, using the necessary intrusion detection mechanisms and authentication mechanisms can prevent detection timely.[3] In the transportation layer of IoT architecture, we analyzed security issues for the access network, core network, and local area network.

Access Network

In access network, we mainly focus on security issues for WI-FI, Ad hoc and 3G-network, and their corresponding solution technologies.

Wi-Fi Security

Wi-Fi stands for Wireless Fidelity. It is a wireless network access specification, also known as IEEE802.11, which is currently the most widely used and very popular wireless networking standards, refers that the wireless terminal can be connected to each other by wireless technology. Wi-Fi based applications in IoT include access the Internet via Wi-Fi web, download or watch online video, etc. When users access the Internet web page, it is feasible to encounter phishing site, users' account and password have to be compromised. Shortly, Wi-Fi security risks mainly include two aspects: first is from the network trap; the second is from the network attack. Wi-Fi security issues are unauthenticated access or attacks. For solving the security issues of Wi-Fi, access control and network encryption are available.

Ad Hoc Security

Wireless Ad hoc network is a group of autonomous wireless nodes or terminals cooperated and formed, independent of the fixed infrastructure which use of distributed network management, who is a self-creating, self-organization and self-management network. Ad hoc networks have the following security issues:

Illegal Node Access Security

Each node needs to be able to confirm or verify the identity of other nodes that communicate with the node, otherwise, an attacker can easily capture a node, thus allowing access to critical resources and information, and to interfere with other communication nodes. So, authorization and authentication can address this security issue.

3G Network Security

3G networks have several security problems: user information leakage, data incompleteness, illegal access attacks and other security issues. Nonpublic information by the user, the key management mechanism, data origin authentication and data encryption are able to solve the corresponding security issues, but unfortunately, the current security mechanisms are still in the research stage. In the process of data transfer, it consists following issues: data leakage, illegal node access and unlawful attacks. By using the appropriate security key management mechanisms, behavioral entity authentication can resolve these issues.

Core Network

Core network of IoT is generally responsible for the data transmission. In the Internet, a large number of nodes need to access to the Internet, which requires a lot of IP addresses, the traditional IPv4 based Internet is unable to meet so many sensor nodes, so the next generation Internet based on IPv6 can solve this problem.[4] For using IPv6 sensor networks with low power consumption for heterogeneous integration, we can take 6Lowpan technology to solve the problem of IPv6 addresses.

Local Area Network

In IoT, local area network should take data leakage and server's independent protection security issues more intensely. Network access control is to ensure the network resources being used legally or authenticated, which is the main strategy of network security protection. Others, such as refusal of malicious code, closing or deleting unnecessary system services, and constantly updating the operating system patches, using a secure password and the password can be used to protect the security of local area network of IoT.

4 CONCLUSION

This paper focuses on the security problems and how the Internet of Things can help to resolve those problems. This survey paper gives the brief introduction of Internet of Things. We analyzed the security challenges of IoT .We also analyzed the features and security issues of transportation layer, and introduced the corresponding solutions for each security issues. Also we equated security issues between IoT and traditional network, and concluded that IoT system lives in a more dangerous environment with limited resources and less network guards, thus lightweight solutions would always be our first choices for IoT security.

5 REFERENCES

T. Phelan. Datagram Transport Layer Security (DTLS) over the Datagram Congestion Control Protocol (DCCP). RFC 5238, May 2008.

A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D Tygar. Spins: Security protocols for sensor networks. In Wireless Networks Journal, September 2002.

Li, C., & Chen, C. L. (2011). A multi-stage control method application in the fight against phishing attacks. In Proceeding of the 26th computer security academic communication across the country.

Liu, B., Chen, H., Wang, H. T., & Fu, Y. (2012). Security analysis and security model research on IoT. Computer & Digital Engineering.

Said Omar, Masud Mehedi, "Towards Internet of Things: Survey and Future Vision" International Journal of Computer Networks (IJCN), Volume (5): Issue (1): 2013.

Bello Oladayo, Zeadally Sherali, "Intelligent Device to Device Communication in the Internet of Things" IEEE System Journal Vol.10 September 2016.