IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 4 Issue 5, May 2017
ISSN (Online) 2348 – 7968 | Impact Factor (2016) – 5.264
www.ijiset.com

Hardware & Software Security Challenges in Internet of Things: A Review

Sarishka[1], NeetiKashyap[2]
Department of Computer Science& Engineering,
The NorthCap University, Gurgaon, Gurgaon, India[1,2]

Abstract
The term Internet of things (IoT) is defined as the representation of materials and things virtually on internet like structure and was first brought in use in 1998.Internet of Things is playing a major role as it covers all the area from old equipment's to the daily used materials to the WSNs (Wireless Sensor Networks) and RFIDs(Radio Frequency Identification).IoT has great potential to face many upcoming challenges and security is one amongst them.This paper mainly on the security issues in IoT. IoT comprises of both hardware and software so the security in IoT needs to be ensured at both hardware and software level. The structural design of IoT is broadly divided into three parts: perception layer, transportation layer and application layer. This paper classifies security in IoT into two types: Hardware Security & Software Security. By deeply studying and recognizing the features and architecture of security, its requirements are given. This work focus on all the layers as security and privacy should be ensured on all layers, implementing security on a single layer will not satisfy the security needs.
Keywords: Internet of Things, WSNs, RFIDs, Hardware Security, Software Security.
.

1. Introduction

Internet of things is the term that defines connection between devices fixed with software, sensors, electronics, actuators, and network connectivity like physical devices, vehicles, buildings, and other items—that allowthese objects to gather and interchange the data between them[1]. In 2013 the Global Standards Initiative defined the term
IoT referred asInternet of Things as "the building block of the information society." The word IoTwhich is nowadays in trend allows sensing of real lifetime objectsand/or it can becontrolledremotely via already existing network structures. itdirectly links and connects real life world and virtual world .When IoT is linked with sensors and actuators, it creates more opportunities for smart cities,smart grids, homes and digital world. In IoT every object can be recognized uniquely through the fixed computing system but is able to work with already used existing Internet infrastructure. According to the predictions and calculations done by the Experts by the year 2020 IoT will contain more than 50 billion objects. Usually, the major four components of IoT are analysing or sensing, accessed from different components, data an alyzing, applications and services, and other components including security and isolation. According to Anass RGHIOUI[7] : The term IoT referred to as Internet Of Things is a great project whose main focus is to connect devices through the internet to collect and transfer data directly with each other ,to gather, to study and to examine new data streams with more higher rate and with increased accuracy. HuiSuo[4] in year 2012 defined IOT as:IoT that is Internet of Things (IoT) is the term that refers to those items and things that can be uniquely identified and their representations can be done in an internet-like structure virtually, and was projected in the year 1998 . In the upcoming years, the idea of IoTis widely increasing and becoming popular through some representatively smart applications like smart greenhouse monitoring, intelligent transportation, electric meter reading, and telemedicine monitoring etc. The term IoTincyber world is known to a great extent, different applications used in industriesare linked to the IoTand many new applications will arise, for example cyber-transportation systems (CTS), cyber-physical systems (CPS), and machine-to-machine (M2M) communications. In terms of security, the term IoT willface more severe challenges in the upcoming worldbecause of some of the these reasons: 1) the term 'internet' is related by the term 'IoT' through the age old internet, mobile networks and sensor networks 2) the term 'internet' connects each 'thing' differently, and 3) as each of these 'things' communicates with each otherand sogive rise to the new security and privacy issues. Bill Gates mentioned Internet of Things in "The Road Ahead" in year 1995.ITU published theReport in the year 2005 on internet forecasting that it's establishment will increase more than 1 billion times the order of theequipment used for gathering

information, 3 billion of useful electronic devices, five hundred billion times the microprocessors, and according to their information the sensor requires more than few trillions. IoT that is Internet Of Things is of great use in the upcoming information industries in near future, and is an advantage to the information industry in the field of computer networking. How is the term Internet Of Things defined? The term is defined as: Through RFID that is radio frequency identification ,global writing system, infrared sensors, laser scanners and other equipments used for information sensing, connecting any object to the Internet for gathering and exchanging information or data and for communication services in order to have good device locating, tracking, monitoring systems and use the functions of a network in order to integrate the physical infrastructure and IT infrastructure. According to GAN Gang[3]: The term IoT that is Internet of Things is "Materialistic objects connected to the materialistic objects in the Internet." This defines its 2 meanings as follows: 1.Theterm Internet is not only the heart and basis of Internet of things, but is also an extension of the Internet. 2. Client's extension and expansion link things and objects and generate information in order to communicate. Wu Jun[11] defined IOT as: The new structure of internet termed as Internet of Things (IoT) will link various computers, storage devices, data, applications and other resources for successful incorporation, virtualization & abstraction. According to his report computing of resources at a large-scale will provide trustworthy services to users of IoT, which the users from the complexities of the underlying hardware logic, network protocols, software architecture freed. The Internet of Things (IoT) has become the most talked about topic in the top ten IT technologies and its existence has changed the way of recognition of information consumption industry and academia by the people. According to the U.S. Federal Trade Commission as IoT stores the information and data of its users on internet so the security of its users information is not maintained though IoT is an advantage and is of great use to business users and consumers reduce its costs. The point of attention is whether the security of the users information stored on internet via IoT must be compromised or not. The two great challenges of IoT that exist and need to be dealt with as soon as possible are: Security and privacy issues.

2. RELATED WORK

Xiong Li et al 2011[2] explained the secure structural design related to IoT, whose main focus was on the user components. JIANG Jun[3] et al 2011 defined Internet of Things as a small piece of area with small-scale and self-obtained satisfactory success and bright future. His main aim was to focus on the Internet of Things application in the country and even in the upcoming years, he analysed the already existing security issues in IoT related to network and transformation of data. Hui Suoa et al 2012[4]discussed some important technologies research status like encryption mechanism, communication security, protecting sensor data and cryptographic algorithms. He focussed on security and privacy in IoT, and examined the features and requirements of security on the four layers of IoT. Kai Zhao et al 2013[5]described the security related problems of the term Internet of Things (IoT). They are directly linked to the applications of its system. The IoT development is an important part of IoT security according to him .He generated few problems from different layers and solutions to those problems for each layer of IoT security structure. Jing et al 2014 [6]discussed the issues related to security in IoT and described in detail the cross-layer mixed combination issues, and he tried to find out reliable solutions to the security related problems. His main focus was on the structural design of security and issues related to security of IoT. According to his study IoT must be divided into three layers: perception layer, transportation layer and application layer. His study of the features and security related issues of IoT helped him introduce new and some typical solutions to those issues. Moreover, he compared the features of the different solutions provided by him by studying and learning the technology involved. Anass Rghiouiet al 2014[7]issued a security model and solutions related to IoT besides presenting a study related to the potential security problems. His model is based on symmetric cryptography with a proposed key management system and network nodes authentication mechanism. He presented a security model to secure an IoT healthcare monitoring system.

3. IoTSECURITY

Security and privacy are the two main issues to be worked upon to make IoT a wide approach in the near future. They should not be dealt in an old fashioned manner and using ad-hoc approaches. A proactive approach is required, where fidelity is engineered up front into IoT. Strong security foundation should be built for IoT and its related components. Measures must be taken and must be implemented to address the reality and upcoming challenges of data origin, data integrity, identity management, trust management, security and privacy issues. The absence of strong security foundations leads to attacks and malfunctioning in the IoT related devices and will decrease any of its uses. The security and privacy of information and network should be fixed with these properties such as detection, secrecy, integrity and undesirability in order to have secure networks. Unlike

internet, the IoT can be used for the most important areas of national economy for e.g., healthservices, medical care, smart shipping and thus the security needs in the IoT will be high in accessibility and reliability. Applying security onto a single layer is not sufficient so security should be applied to different layers according to the need and requirement. The four main key challenges to design a secure IoT network are :

- **Data origin and reliability:** Reliability is producing same results under same consistent situations. Data collected from different origins is rarely consistent because of the accuracy or non-response.
- **Identity management:** It is the management of users identity and personal information within the system boundaries for security and privacy reasons.
- **Trust management:** It is a system used in the world of technology to ensure security of social trust usually to have automatic decision making system
- **Security:** It refers to the maintenance of privacy and ensuring data and system security.

Information derivation considers that the data collected is from a reliable source. Malicious attack on the data must be taken care of by the data reliability. The trust in the devices must be ensured by Trust management. Identity management refers to the administration of individual identities. Privacy is necessary to ensure that the user's information, personal detail, his data and his credentials are only under his control and no one else is able to access it or work upon or change them. The IoT security desiderata can be grouped into two broad classes. The first class consists of Hardware Security and the second class consists of Software security.

4. HARDWARE SECURITY

To build a secure IoT implanted and hardware security is also required. To secure the resource-controlled implanted devices such as to collect the information the sensors are used, the processing of information is done by the nodes, and to perform the physical action actuators are required.1.ThePUf technology is used to integrate the sensing, data provenance and integrity. 2. PUFs are used for identity management.3.For trust management and data privacy we use we use hardware performance counters.4.lightweight cryptography must be used to ensure privacy. In the field of IoT the major issue considered is data privacy which guarantees the access of only authorised data. Specifically it is used for the business framework, where the data is used to represent an entity to protect and to secure competition and advertising ethics. The data In the IoT must be modified by both the users and the registered objects. The two major constraints to be considered are:

1. How an access based mechanism must be controlled can be defined and
2. The description of an object verification process (with a related identity management system).

In Internet of Things that is IoT environment information is generally based on the physical layer that ensures information security as an important factor for many cases). For example, we will regard data recorded by bio-sensors on making of the bacterial products required for ensuring quality food. The data collected is protected as its spreading is a threat for company's reputation. As of example two, we may now observe an environmental monitoring application, where information collected is used to issue warnings before the occurrence of disasters like tsunami/earthquakes etc. the civil protection bodies should only keep this data in order to ensure there use for future strategies to control disaster. The spreading of this data to the local citizens might create mess and chaos, putting the lives of common people at risk. Appropriate solutions for securing data cannot be directly applied to IoT applications, because of the two major reasons. The first one considers the utter amount of data and information generated by such systems, and relates hence to scalability issues. The second reason is: It considers the requirement of scheming and accessing the information in much easier way with rights to access and modify data at run-time.

4.1 LIMITATIONS BASED ON HARDWARE.

1) Computational and energy constraint: IoT devices are mostly driven by battery which uses low-power CPU's that have comparatively low clock rate. Thus, the algorithms that require fast computing that is computationally expensive cryptographic algorithms cannot be directly altered to these devices that are low powered.

2) Memory constraint: In comparison to the traditional digital systems (e.g. PC, Laptop, etc.), IoT devices nowadays generally ,have low RAM and Flash memory and they use Real Time Operating Systems (RTOS) or the lightweight version of General Purpose Operating System (GPOS). System software and proprietary services are also ruined. Thus, memory proficient protection schemes should be used as the traditional digital system uses large RAM and hard drive. Those security schemes might not get enough space in memory after booting up the operating system and system software. Therefore, IoT cannot be secured by using usual security algorithms.

3) Tamper resistant packaging: IoT devices might be ignored and deployed in the far-off regions. An attacker might control the IoT devices and interfere with them.

They can take out the cryptographic secrets, update or modify some of the programs, or replace them with malware and virus affected nodes. Packaging opposed to tamper is one way to protect IoT against these attacks. Threats handled by hardware security include:

1. Configuration management: It is a system that ensures the consistency of performance of a product, its functional and physical components according to products requirement, its design and performance.
2. Auditing & logging: It is a set of records that contains security details and also the details of activities that have cause threat to a particular event or procedure at any point of time.
3. Query string manipulation: It helps in manipulating and parsing issues and queries related query strings.

5.SOFTWARE SECURITY

As software is complex and not directly accessible by the user so it is often regarded for errors, cyber malfunctioning and so it is quite difficult to completely prevent this layer from disturbances and virus attacks etc. These complexities will increase with the IoT and can't be protected from. Because of the complexity of software this layer is the most difficult to be protected from the virus attacks and threats etc and so ensuring its security becomes necessary.

5.1 SOFTWARE SECURITY LIMITATIONS

1) Embedded software constraint: IoT devices are generally installed in the Operating Systems based on IoT that have small size networking protocol stacks and may not contain many devices for security. Thus, the devices designed for security should have thin, rough and fault bearable protocol stacks.

2) Dynamic security patch: Installing the dynamic security patches on the devices in IoT layer and reducing the potential liabilities is not an easy task. In IoT devices remote programming is not possible because the operating system or protocol stack may not be able to accept and incorporate new code or library.
Software security can handle threats like: .Input validation, Buffer overflow, Eaves dropping/data tampering, Session hijacking, MITM.

6. SECURITY IN VARIOUS LAYERS OF IoT

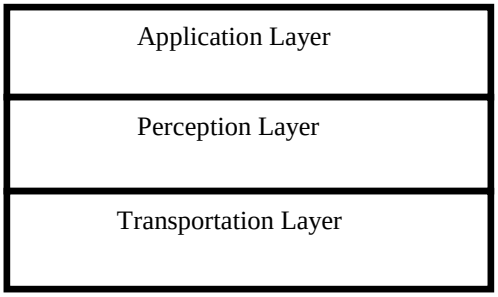
The layers of IoT are defined as below:

1.PERCEPTIONLAYER**:** Perceptual Layer is the most basic kind of layer. It gathers different kind of information from different sources using different machines and equipment and it identifies the data from the physical world. The gathered information includes different kind of object properties, environmental condition etc., and the physical equipment include RFID i.e. radio frequency identification readers, different types of sensors, GPS and other equipment. Sensors are the main element of this layer that captures the data and represents the material or physical world into the digital world. This layer is responsible for sensing, perceiving and transmitting data to other layers. This layer comprises of various sensor devices such as temperature sensor, humidity sensor, camera to capture images etc. These devices help in capturing data which further is utilized by various applications in the application layer.[12]13]

2. NETWORKINGLAYER**:** This is the second layer under architecture of IoT. This layer includes Encryption mechanism, Communication security and Anti-dos. This layer works for and helps in the easy broadcasting of data from first layer i.e .perception layer to the early processing of data, its categorization and polymerization. This layer includes various mechanisms responsible for transmission or dissemination of information to the Application layer. Various communication system technologies such as Wifi, Wifimax and so on are part of this layer. It also contains various stacks of communication protocols which help in successful and good quality communication.

3.APPLICATION LAYER**:** This is the third and the top most layer in the architecture of IoT. Application layer is the most broadly classified layer amongst all other layers in IoT. It provides the use according to the need of the users. IoT can be easily accessed through the this layer by use of devices like TVs, Computers or other equipment like mobile and so on. Use of IoT is increasing these days and so there is an urgent need for securing and encrypting this layer.

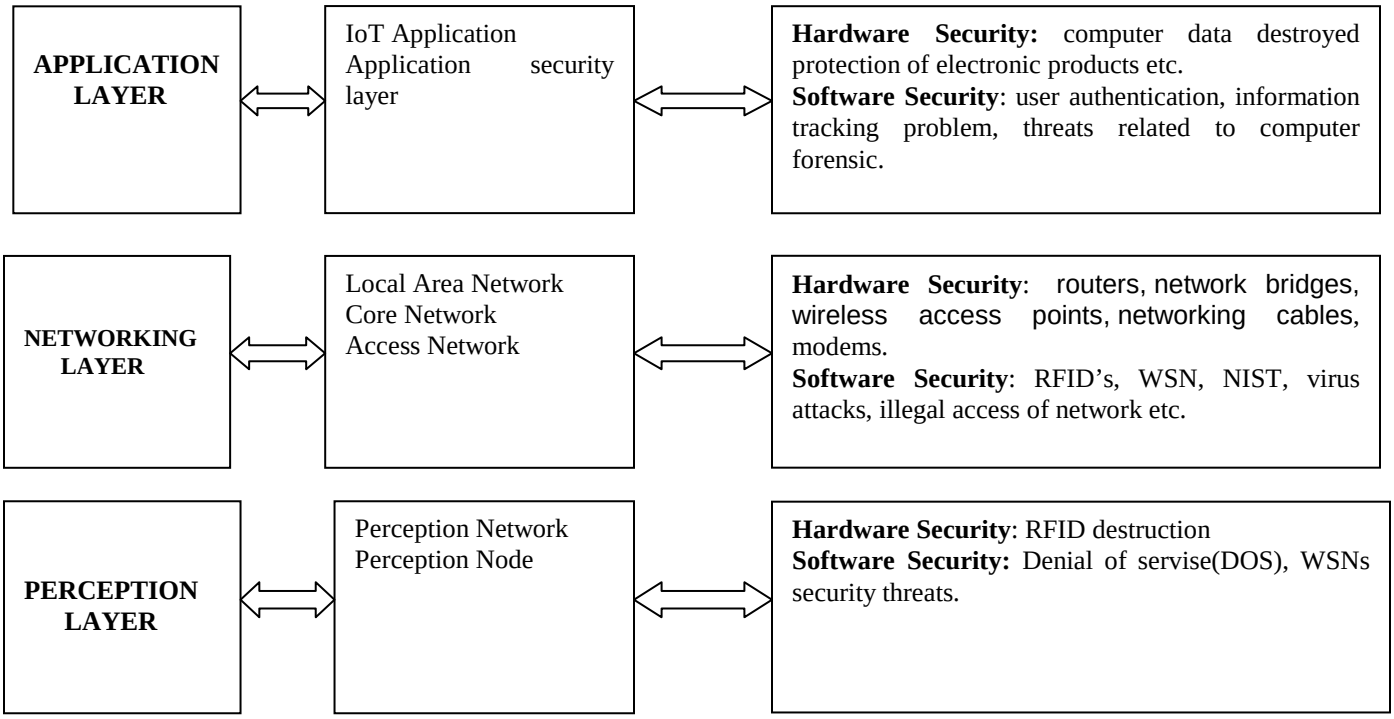
Fig1. Layered Architecture of IoT



Various methods are used to secure and encrypt this layer but still some more advance methods are needed in order to secure this layer. Its open ended nature may be the reason for some of the threats. Some of the threats are summarized as follows:

1. The low and non-existent security design is the first basic threat to the Application Layer the normal working of an application.
2. Some applications store some of the secret and sensitive information in the publically accessed files like HTML code of a web form or encode it in "hidden" areas which are not displayed to common man.
3. Some of the programs have some well-known shortcuts that are known by some other secure controls and are unauthorized accessed. Applications that have no authentication or weak authentication are more often used in unauthorized way.
4. Applications may depend upon some untrusted channels to gain the identity or set the privileges.

Fig 2: Various Security Threats



7. Conclusions

In this paper our focus was on Hardware and Software security issues on different layers of IoT divided as: Perception layer, networking layer, and Application layer. We studied some of the hardware and software features of security on different layers. We also provided key issues based on the development of IoT ideas and technologies. IoT has connected millions of devices and so ensuring its security is a necessity. The use of IoT devices will in one way or other increase the use of computers and even link and increase the use of mobile phones by several more times.

8. References

1. Gubbi, Jayavardhana, et al. "Internet of Things (IoT): A vision, architectural elements, and future

directions." Future generation computer systems 29.7 (2013): 1645-1660.
2. Li, Xiong, Zhou Xuan, and Liu Wen. "Research on the architecture of trusted security system based on the internet of things." Intelligent Computation Technology and Automation (ICICTA), 2011 International Conference on. Vol. 2. IEEE, 2011.
3. Gan, Gang, Zeyong Lu, and Jun Jiang. "Internet of things security analysis." Internet Technology and Applications (iTAP), 2011 International Conference on. IEEE, 2011.
4. Suo, Hui, et al. "Security in the internet of things: a review." Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on. Vol. 3. IEEE, 2012.
5. Zhao, Kai, and Lina Ge. "A survey on the internet of things security." Computational Intelligence and Security (CIS), 2013 9th International Conference on. IEEE, 2013.
6. Jing, Qi, et al. "Security of the Internet of Things: perspectives and challenges." Wireless Networks 20.8 (2014): 2481-2501.
7. Rghioui, Anass, et al. "The Internet of Things for healthcare monitoring: Security review and proposed solution." Information Science and Technology (CIST), 2014 Third IEEE International Colloquium in. IEEE, 2014.
8. Xu, Teng, James B. Wendt, and Miodrag Potkonjak. "Security of IoT systems: Design challenges and opportunities." Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design. IEEE Press, 2014.
9. Abomhara, Mohamed, and Geir M. Køien. "Security and privacy in the Internet of Things: Current status and open issues." Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on. IEEE, 2014.
10. Hossain, Md Mahmud, Maziar Fotouhi, and Ragib Hasan. "Towards an analysis of security issues, challenges, and open problems in the internet of things." Services (SERVICES), 2015 IEEE World Congress on. IEEE, 2015.
11. Chen-wen, WANG Jian-qiang WU, and L. I. Xiao-jun. "Research on Architecture and Key Technologies of Internet of Vehicles [J]." Microcomputer Information 4 (2011): 067.
12. NeetiKashyap "Era To Move From Internet Of Things To Web Of Things.", International Journal of Advance Foundation and Research in Computer, Volume 3, Issue 4, 2016.
13. SakshiGarg, NeetiKashyap, Hitesh Yadav, Energy Harvesting Techniques in Internet of Things-A survey**,** International Journal of Innovative Science, Engineering and Technology, Volume 4, Issue 2, February 2017.