IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 11-16

A Review On Security Of Technologies of IoT

Sushree Priyanka Mishra[1],Ankeet Agarwalla[2],Jayasmita Mohapatra[3], Neelamani Samal[4]

[1](Department of CSE-CTIS, Inurture Education Solutions Pvt. Ltd. India, CUTM, India)
[2](Department of CSE-CTIS, Inurture Education Solutions Pvt. Ltd. India, CUTM, India)
[3](Department of CSE-CTIS, Inurture Education Solutions Pvt. Ltd. India, CUTM, India)
[4](Department of Computer Science & Engineering, Biju Pattnailk University Of Technology,India)

Abstract:*This paper provides an overview of the Internet of Things (IoT) that which facilitates daily activities and the devices are connected through the Internet. IoT allows that device to be sensed and controlled remotely by maintaining proper connection among the devices. Through IoT data can be transferred over internet with minimal human intervention. The back bone of IoT includes various communication protocol, technology used for the communication, standards, operating system, software, hardwares*
In this paper we have also discussed about the architecture and technology used in IoT.This paper is a survey of most common technologies used in IoT such as RFID ,RFID Reader,NFC,IP.
We have also discussed about the goals of Information security ,Common threats and solution for the Technologies like RFID ,NFC and Mobile.

***Key word** :RFID,NFC,Mobile,Security*

I. Introduction to IoT

The term IoT has been developed for few years. The basic idea of this concept is the presence of a variety of objects such as RFID, NFC, sensors, actuators, mobile phones. TheInternet of things is the network of physical devices and other items embedded with electronics, soft wares, sensors, actuators, and connectivity which enables these things to connect and exchange data and creating more opportunities for direct integration of the physical world into computer based environment.

In this IoT technology RFID is the most important concept and it is necessary for IoT. But the main problem IoT facing is the security problems. The IoT specifically refers to the coding and networking of physical objects and things to make them machine-readable and traceable on the Internet of Things that has been created through coded RFID tags.

IoT Architecture

The IoT can be capable of interconnecting various heterogeneous objects through the Internet so there is a need for a flexible layered architecture to avoid the occurrence of any type disruptions in the operations.
The basic model is a three layered architecture consisting of the Application, Network and Perception layers.

Object layer: The first layer is object or perception layer and it represents the sensors in form of RFID tags, IR sensors or other sensor networks and actuators used in IoT that is used to collect and process information. The sensors and actuators perform different types of functions such as identifying temperature, motion, location, weight, acceleration etc. This layer digitizes and transfers data to the Object Abstraction layer through a secure channel.Then the digital signal is passed to the network layer.

Object Abstraction Layer: It transfers data to the Service Management layer that are produced by perception layer or object layer via the secure channels. Data can be transferred using RFID, 3g, Wi-Fi, Bluetooth etc. Cloud computing and data management processes are also carried out in this layer.
Service management layer: The next layer is service management layer .This layer pairs a service with its corresponding requester based on their addresses and names. Service Management layer also allows the IoT application programmers to work with heterogeneous objects without any considerations to a specific hardware platform. Information received from sensor devices is processed by this layer.
Application layer: This layer provides the services requested by customers. It is very helpful in the large scale development of IoT network. It is the top most layer which provides business logics, formulas, and UI to end users.
Business layer: This layer manages the overall IoT system services and activities. Business layer builds a business, model, graphs, etc. based on data received by application layer. It also implements, designs, monitor, analyse and develop the elements related to IoT. Business layer also monitors and manages the underlying four

layers. It also compares the output of each layer with expected output to improve the services for effective business strategies.

Technologies Used in IoT

There are several technologies that can be used to implement the concept of Internet of Things. In this paper we have discussed about the following technologies:

- **RFID(Radio Frequency Identification Device)**
- **RFID Reader**
- **Internet Protocol**
- **NFC(Near Field Communication)**

1. RFID: The RFID is a unique identity of object or person wirelessly using radio waves in the form of numbers. FID technology plays an important role in Iot for solving identification issues. FID system is composed of one or more reader and several RFID tags. Tags uses radio frequency electromagnetic field to transfer data attached to an object.

The tags contain electronically stored information. The RFID device serves the same purpose as a bar code or a magnetic strip on the back of a credit card or ATM card.It provides unique identifier for each object.

2.RFID Reader: A radio frequency identification reader is a device used to gather information from an RFID tag, which is used to track individual objects. Radio waves are used to transfer the data from the tag to a reader. The RFID tag must be within the range of an RFID reader which ranges from 3 to 300 feet.

3. Internet Protocol: It is the primary network protocol used on the internet. The two versions of IP are: IPv4 and and IPv6.Each version defines the IP address differently. There are 5 classes available in in IPv4 are: class A, class B, class C, class D, class E.

4. NFC: NFC has the features and functionality to be a key enabler of IoT devices and foster wide scale adoption.NFC can put IoT devices under a user's control,is easy-to-use with its "tap and go" functionality and provides a number of security options.NFC provides four key capabilities that will move IoT to wide scale adoption.

- **The ability to connect the unconnected**
- **User control with expressed intent**
- **Easy network access and data sharing**
- **Data security at multiple levels**

Threats and Solution of IoT devices

In this section security issues of different IoT technologies are discussed . IoT devices are vulnerable to different kinds of threat due to diversity,weak protective capabaility of sensing node such as RFID NFC and Mobile. As internet is key infrastructure of IoT so there is a possibility of security challenges that is faced. Some of the security attack along with the solutions are elaborated in this section. This section is divided to two main aspect as given below:

1) Principle of Secuirty
2) Threats & Solution and Recomendation of IOT devices such as RFID ,NFC and Mobile are discussed

Principle of Secuirty :

The main goal of security requirements includes:

Confidentiality : Secure the data from unauthorised access

Integrity : It ensures correctness of data

Availability :Data should be available at right time to the right users

The three principle of Security can be represented by using CIA triad as shown below

CONFIDENTIALITY
AVAILABILITY
CIA
TRIAD
INTEGRITY

Figure:1 CIA Triad

As goal , Security provides confidentiality, Integrity and Availability so the security requirement for IoT is the major concerns.

II. Threats & Solution of IOT devices

2.1 RFID

Description: RFID technology is mainly used as RFID tags for automated exchange of information without any manual involvement.

Threat

The four most common types of attacks and security issues of RFID tags are as follows:

i. Unauthorized tag disabling: In this DoS attacks the RFID tags will become incapable temporarily or permanently. Such attacks make RFID tag available to malfunction and misbehave under the scan of a tag reader. These attacks can be done remotely, allowing the attacker to manipulate the tag behaviour from a distance.

ii. Unauthorized tag cloning: Capturing the identification information through the manipulation of the tags by dishonest readers falls under this category. Once the identification information of a tag is compromised, replication of the tag is made possible which can be used to bypass fake security measures as well as introducing new vulnerabilities using RFID tags automatic verification steps .

iii. Unauthorized tag tracking: The dishonest readers can trace the tag, which results in giving the sensitive information, for example person's address. Thus from the viewpoint of customer, buying a product which is having an RFID tag guarantees them no confidentiality regarding the purchase of their chase and in fact endangers their privacy.

iv. Replay attacks: In Replay attacks the attacker uses a tag's response to a dishonest reader's challenge to impersonate the tag. In this attacks, the communicating signal between the reader and the tag is intercepted, recorded and replayed upon the receipt of any query from the reader at a later time, thus faking the availability of the tag

Table-1 :Threats of RFID device :

Name of Threat	Threat to
Unauthorized tag disabling	This is Threat to confidentiality
Unauthorized tag cloning	This is Threat to Integrity
Unauthorized tag tracking	This is Threat to Confidentiality
Replay attacks	This is Threat to Availability

Solutions & Recommendation for RFID :

As per the above security threats for the RFID here will discuss about the solution.The counter measures to prevent the IoT based on RFID includes :

The disabling attack. In a disabling attack the attacker causes tags to assume a state from which they can no longer be identified by the back-end server. One way to prevent this is by having each tag share with the server a permanent (non-erasable) private identifying key

ktag (another way, which is however not suitable for low-cost tags, would be to use publickey cryptography). Then, when a tag is challenged by a reader, it will generate a response using this private key. Of course, it should be hard for an attacker to extract the private key from the tag's response. For this purpose a cryptographic one-way function should be used.

This solution relies heavily on the assumption that the server is trusted and physically secured.

The cloning attack. To defeat cloning attacks it should not be possible for an attacker to access a tag's identifying data. Such data should be kept private. However for authentication,it should be possible for the back-end server to verify a tag's response. The response must therefore corroborate (but not reveal!) the tag's identifying data. This can be achieved by having the server share a private key ktag with each tag, as in the previous case.

The tracking attack. Unauthorized tracking is based on tracing a tag responses to a particular tag. This can be prevented by making certain that the values of the responses appear to an attacker as random, uniformly distributed. In fact, since we are assuming that all entities of an RFID system have polynomially bounded resources, it is sufficient for these values to be pseudo-random.

Replay attacks. To deal with replay attacks the tag's response must be unique for every server challenge. To achieve this, the values of the server challenges and the tag responses must be unpredictable. One way to achieve this is to enforce that the answers be

(cryptographically) pseudo-random

2.2 NFC :

Description : Near-field communication (NFC) was introduced in the year 2002 by both sony and Philips.In this technique it allows any two electronic devices which have NFC in them to communicate with each other in a

close proximity i.e within a range of 20 cm.NFC is a wireless communication interface .The interface operates in several modes.The different modes are based on RF fields which are stated below :
1.Active Device::In this case if the device generates its own RF field
2.Passive Device : In this case if the device retrieves the power from RF field that is generated by another device
The two devices can communicate in different communication configuration as listed in the table:

Table-2 Communication Configuration of NFC device

Device A	**Device B**	**Description**
Active	Active	RF field are generated by both Device A and Device B
Active	Passive	The RF field is generated by Device A only
Passive	Active	The RF field is generated by Device B only

The way of data transmission depends on modes i.e Active mode or Passive Mode of transmitting device.
It can be applied in IoT for providing wide range of services such as Payments, Authentication ,Data Exachange etc

Threats of NFC :
The most common Threat to NFC are as follows :

Eavesdropping : As NFC is wireless communication interface ,so in this case when two device communicate with each other via NFC using RF waves then the attacker can use the antenna to receive the transmitted signal.
In case of the sender device is in Active mode then the eavesdropping can be done up to a distance of about 10 m,While when the sending device is operating in Passive mode this distance is significantly reduced to about 1 m. Also it is harder harder to eavesdrop on devices sending data in passive mode.

Denial of Service Attack : NFC is more prone to DOS attack. In this case the attacker send valid frequency so that the receiver is unable to understand the data transmitted by the sender. In this case the attacker trigger expensive operation that consumes resources such as network bandwidth, computational power,memory.

Data Modification and Corruption : In this case the attacker instead of just listening can modify the data by sending some valid frequency spectrum at the right time. The calculation of the right time is possible if the attacker has good understanding of modulation scheme and coding.

Data Insertion : This is the process of inserting message between two communicating device.This is only possible, if the answering device needs a very long time to answer. The attacker could then send his data earlier than the valid receiver. The insertion will be successful, only, if the inserted data can be transmitted, before the original device starts with the answer. If both data streams overlap, the data will be corrupted.

Man in the Middle Attack
In this case when Alice sends any data to Bob then the message is attacked by the third party Eve .Alice and Bob are not aware that they are sending and receiving data from Eve.

Table-3 :Threats of NFC device

Name of Threat	Threat to
Eavesdropping	This is Threat to confidentiality
DOS	This is threat to Availability
Data Insertion	Threat to Integrity
Data Modification/Corruption	Threat to Integrity
Man in the Middle Attack	Threat to Integrity

Solution and Recommendation of NFC device :
In the section we have discussed about the possible solution and recommendation to protect the threat **.**
Eavesdropping : To protect the Eavesdropping secure channel is required to established for data exchange
Data Corruption : In this case the NFC device can detect the RF field while data transmission. This leads to detect the attacker
Data Modification :
There are different methods to prevent the Data Modification attack as explained below:
i)By using 106k Baud in active mode it gets impossible for an attacker to modify all the data transmitted via the RF link. This means that for both directions active mode would be needed to protect against data modification.

ii)NFC devices can check the RF field while sending. This means the sending device could continuously check for such an attack and could stop the data transmission when an attack is detected.

iii)The third and probably best solution would be a secure channel

Data Insertion:

There are three possible countermeasures.

1. One is that the answering device answers with no delay. In this case the attacker cannot be faster than the correct device.
2. The second possible countermeasure is listening by the answering device to the channel during the time, it is open and the staring point of the transmission. The device could then detect an attacker, who wants to insert data.
3. The third option again is a secure channel between the two devices.

Man in the Middle attack :

The active party should listen to the RF filed while sending data to be able to detect any disturbances caused by a potential attacker.

The recommendation is to use active-passive communication mode such that the RF field is continuously generated by one of the valid parties

Secure Channel :

Establishing secure channel between the sender and receiver is the best approach to prevent against attack like eavesdropping and any kind of modification attack. The secure channel ensure to provide confidentiality ,integrity, authentication while data transmission.

Secure channel can be implemented by using cryptographic technique such as 3DES or AES based on standard key agreement protocol.

2 .3 Mobile :

Description: Many IoT devices as wearable devices and smart cars are used in the mobile environment. These mobile devices often need to hop from one network environment to another environment and have to communicate with many unknown new devices. For example, use drive smart car from one district to another, the car will automatically collect road information for highway foundational facilities in the new district. This scenario will be more common in the future of social IoT. We describe the movement of IoT devices as an IoT feature named “mobile” here.

Threats of Mobile Device:

Injection of Malicious code : Because mobile IoT devices are more likely to join more networks, hackers tend to inject the malicious code into mobile IoT devices to accelerate the spread of malicious code.

Table-4 :Threats of Mobile Device

Name of Threat	Threat to
Injection Of Malicous Code	This is Threat to confidentiality

Solution & Recommendation of Mobile Device :

The threat on mobile device can be reduced by dynamically changing the configuration of device according to the trust condition other device in different network .

III. Conclusion

Considering the limitations and drawbacks of the physical solutions for providing security and privacy in RFID, NFC applications, these solutions are suitable for particular applications and cannot be applicable for all . Other solutions are required that does not suffer any limitation on the communication process as well as on the threat handling mechanisms such . A list of threats has been derived and addressed. NFC by itself cannot provide protection against eavesdropping or data modifications. The only solution to achieve this is the establishment of a secure channel over NFC. This can be done very easily, because the NFC link is not susceptible to the Man-in-the-Middle attack. As the mobile device operates is cross platform domain i.e mobile hops from one domain to another so configuration of device needs to change dynamically to reduce the probability of attack. These limitations makes a challenge in our IoT implementation and need more secure protocols for its massive implementations.

References

[1]. [1] Jun Wei Chuah ―The Internet of Things: An Overview and New Perspectives in Systems Design‖ 2014 International Symposium on Integrated Circuits 978-1-4799-4833-8/14.

[2]. [2] Sarita Agrawal, Manik Lal Das ―Internet of Things – A Paradigm Shift of Future Internet Applications‖ Institute of technology, nirma university, ahmedabad – 382 481, 08-10 december, 2011.

[3]. [3] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari and Moussa Ayyash ―Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications‖ ieee communication surveys & tutorials, vol. 17, no. 4, fourth quarter 2015.

[4]. [4] M.U. Farooq, Muhammad Waseem, Sadia Mazhar, Anjum Khairi and Talha Kamal ―A Review on Internet of Things (IoT)‖ International Journal of Computer Applications (0975 8887) Volume 113 - No. 1, March 2015.

[5]. [5] Tuhin Borgohain, Uday Kumar and Sugata Sanyal ―Survey of Security and Privacy Issues of Internet of Things‖

[6]. [6] Krushang Sonar, Hardik Upadhyay ―A Survey: DDOS Attack on Internet of Things‖ International Journal of Engineering Research and Development e-ISSN: 2278-067X, p-ISSN: 2278-800X Volume 10, Issue 11 (November 2014), PP.58-63.

[7]. [7] Prabhakaran Kasinathan, Claudio Pastrone, Maurizio A. Spirito and Mark Vinkovits ―Denial-of-Service detection in 6LoWPAN based Internet of Things‖ 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob).

[8]. [8] QuandengGOU, Lianshan YAN, Yihe LIU and Yao LI ―Construction and Strategies in IoT Security System‖ 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing.

[9]. [9] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva ―Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues‖ ieee communication surveys & tutorials, vol. 17, no. 3, third quarter 2015.

[10]. [10] Qi Jing • Athanasios V. Vasilakos • Jiafu Wan • Jingwei Lu • Dechao Qiu ―Security of the Internet of Things: perspectives and challenges‖ Wireless Netw DOI 10.1007/s11276-014-0761-7.

[11]. [11] A Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks‖ [Deng+].

[12]. National Cholesterol Education Program (NCEP) Expert Panel on Detection, Evaluation, and Treatment of High Blood Cholesterol in Adults (AdultTreatment Panel III) Third report of the national cholesterol education

[13]. program (NCEP) expert panel on detection, evaluation, and treatment of highblood cholesterol in adults (adult treatment panel III) finalreport. Circulation. 2002;106(25, article 3143).

[14]. Bener A, Zirie M, Janahi IM, Al-Hamaq AOAA, Musallam M, Wareham NJ.Prevalence of diagnosed and undiagnosed diabetes mellitus and its risk factorsin a population-based study of Qatar. Diabetes Research and Clinical Practice. 2009;84(1):99–106.

[15]. Bener A, Zirie M, Musallam M, Khader YS, Al-Hamaq AOAA. Prevalence ofmetabolic syndrome according to adult treatment panel III and internationaldiabetes federation criteria: a population-based study. Metabolic Syndrome

[16]. and Related Disorders. 2009;7(3):221–230

[17]. Bener A, Dafeeah E, Ghuloum S, Al-HamaqAOAA.Association between psychological distress and gastrointestinal symptoms in type 2 diabetes mellitus. World Journal of Diabetes. 2012;3(6):123–129

[18]. Brunzell JD, Davidson M, Furberg CD, et al. Lipoprotein management inpatients with cardiometabolic risk:consensus statement from the American diabetes association and the american college of cardiology

[19]. foundation.Diabetes Care. 2008;31(4):811–822

[20]. Colhoun HM, Betteridge DJ, Durrington PN, et al. Primary prevention of cardiovascular disease with atorvastatin in type 2 diabetes in the collaborative atorvastatin diabetes study (CARDS): multi centrer trial. The Lancet. 2004; 364(9435) :685–696.

[21]. Shepherd J, Barter P, Carmena R, et al. Effect of lowering LDL cholesterol substantially below currently recommended levels in patients with coronary heart disease and diabetes: the treating To new targets (TNT) study.Diabetes Care. 2006;29(6):1220–1226.

[22]. American Diabetes Association.Standards of medical care in diabetes. Diabetes Care. 2009;32(supplement 1):S13–S61.

[23]. Henry RR. Preventing cardiovascular complications of type 2 diabetes: focus on lipid management. Clinical Diabetes.

[24]. Jones PH, Davidson MH, Stein EA, et al. Comparison of the efficacy and safety of rosuvastatin versus atorvastatin, simvastatin, and pravastatin across doses (STELLAR* trial) American Journal of Cardiology.2003;92(2):152–160.

[25]. Group EUROASPIREIIS: Lifestyle and risk management and use of drug therapies in coronary patients from 15 countries.

[26]. Principal results from EUROASPIRE II. Eur Heart J 2001,22:554-572.

[27]. Schuster H, Barter PJ, Cheung RC, Bonnet J, Morrell JM, Watkins C, Kallend D, Raza A, for the MERCURY I Study Group: Effects ofswitching statins on achievement of lipid goals: MeasuringEffective Reductions in holesterol

[28]. Using Rosuvastatin Therapy (MERCURY I) study. Am Heart J 2004,147:705-713.

[29]. Pharmaceutical Management Agency. Prescription for pharmacoeconomic analysis: methods for cost-utility analysis.