International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 10
ISSN: 2454-4248
126 – 130

Internet of Things Security Attacks Research Challenges and Security Requirements

Rajendar Kumar
Department of Computer Science,
Faculty of Natural Science,
Jamia Millia Islamia, New Delhi, India
rkumar1@jmi.ac.in

Abstract - Internet of Things(IoT) the fastest growing technology that is attracting everybody. IoT making life of Human beings better than before, but with this it is also generating some security issues for them. Internet of Things is bringing both human and machine at the common platform that Internet, IoT connect physical devices like Fridge, T.V, vehicle, wearable device etc through internet. Today people are able to control their device from remote areas only through IoT which use sensor to sense data from the environment and transmit that data at the server or cloud where it is not safe. So this paper describes security requirements along with the security attacks that can occur inIoT systems and providesimportant research challenges and future directions in the field of security of IoT system.

Keywords: *IoT(Internet of Things), Cryptanalysis Attacks, heterogeneous devices, Network Attacks, Sensor, security requirements.*

*****

I. INTRODUCTION

IoT is one of the existing technology which is going to familiarized among all the people of all the countries. Today most of the people know about the Internet of things (IoT) and everyone want to opt this new technology to make their life fast and easy. In Fig 1. few applications of IoT is shown and It is expected that the size of IoT market in Europe is estimated to reach €242,222 million by the end of 2020. Today about 23 billon IoT devices are connecting the world and it is expected to reach 30 billion by the year 2020 and 60 billion up to the year 2025. Such large amount of IoT devices will produce too much amount of data that will be available over the internet which will be very difficult to manage and secure. Today, most of the companies or organizations are concentrating on the manufacturing of IoT devices but they are not thinking about the security of IoT data which is the most important aspect of IoT.

Fig 1. IoT Applications

- *Architecture of IoT*

IoT is the fastest growing technique in the field of Information technology, that is connecting many devices to each other at any time from anyplace by using a service or network, but to do so we need a big architecture which can make these things to send data to a common platform like cloud from where any other device can access that data. For every device need some hardware and IoT architecture defines all the necessary components that required for establishing an IoT environment. An IoT architecture consists of four layers: Perception layer, Network Layer, Support layer and Application layer.

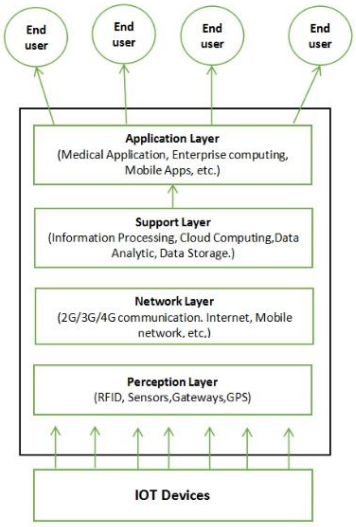

Fig 2. IoT Architecture

All these layers play a vital role in IoT system e.g., Perception layer directly contact with the devices through RFID reader, Sensors, Gateways and GPS. All these devices received data from the things by sensing them. Tagging technology is one of the many techniques which works at this layer and uniquely identifies the different things. Network layer is the second most important layer of IoT system which includes 2G/3G/4G communication network, Internet, Mobile Network, WSN, Optical fibre networks and Broad television network. The main goal of this layer is to send received data from sensors to the information processing system. The third most important layer is Support layer that perform the task of Data storage, Data Analytic and Information processing. Cloud computing is also a important part of this layer which works as a common platform for the all data involve in IoT system. The last layer of IoT architecture is Application layer which is directly in connect of end users. In this layer various application of IoT is

 ISSN: 2454-4248
126 – 130

implemented like Medical Application, Enterprise computing, transportation application and mobile apps etc.

In this paper in Section-II, Literature review will be presented that is done in the field of IoT security. In Section-III, we will discuss about different types of attacks which can be applied on IoT devices to hack them. Section IV, will be based on analysis of IoT attack and finally in Section V conclusion and future scope will be given.

II. LITERATURE REVIEW

Smart devices and low rate internet service attracting most of the people towards the Internet of things (IoT) which is connected all smart devices through internet[1].IoT is allowing the user to control devices from a remote area, for example if you are in your office, then you can control your home appliances like TV, fridge,door,oven, light and many more things. All these devices or things.IoT is connecting devices from simple wearable devices to large machines.IoT devices not only filling our personal need but also providing solutions for community needs, for instance IoT is used in hospital for surgery monitoring, detecting weather conditions, tracking automobiles and tracking animals with the help of biochips that is implemented with animal's body[2].Data that is received by all these devices are processed to get efficient result for IoT environment.

As per literature review, WSNs and M2M or CPS are considered as major components of IoT environment and security issues are also arising with these devices in context of IoT with IP protocols which are the main part of IoT devices connectivity.Hence, It becomes compulsory that entire IoT system must be secured from any type of attack so that in future unauthorized access is not possible for hackers and people can trust on IoT devices.Since all IoT devices connected with each other through a computer internet, hence all security issues of computer network unwillingly come to IoT environment, so we also need to secure our computer network.Alaba et.al [3],In this paper, IoT issues are discussed at application, hardware and network label and issues are categorizing on the bases of application,architecture data and communication. Granjal et. Al [4], discussing and analyzing the IoT protocol's security issues.Sicariet al. [5], give detail of trust management, privacy issues, data security, network security and IDS and except of these author also discussesconfidentiality, security, access control and privacy for IoT along with security for middleware. Zhou et al. [6], giving the detail of location and identity privacy, layer removing or adding, node compromising and key management issues for cloud based IoT.author also discuss the possible countermeasures for different types of IoT issues for cloud based-IoT. Zhang et al. [7], discusses major IoT security issues in terms of unique identification of objects, authentication and authorization, privacy, the need for lightweight cryptographic procedures, malware, and software vulnerabilities.

III. ATTACKS on IoT SYSTEM

IoT is in it's infancy state in which it has to face many types of attacks that makes IoT devices vulnerable, these attacks are shown in Fig.

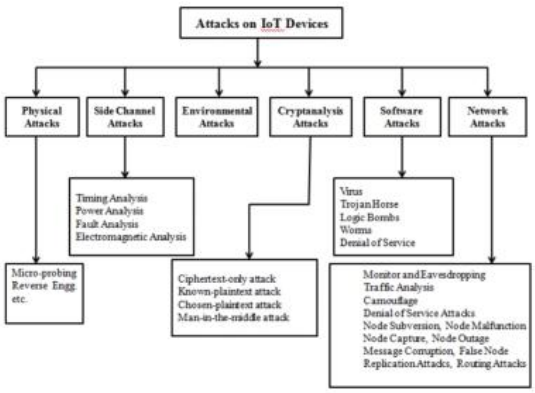

Fig 3. Types of IoT Attacks

i) *Physical Attacks:* Physical attacks are those attacks in which physical devices like Sensors, chips, routers etc. are directly tampered by the hacker to complete his purpose of harming the IoT devices. Layout reconstruction, micro-probing, de-packaging of chip and particle beam techniques are some examples of physical attacks [8].

ii) *Side Channel Attacks:* In this type of attacks information is extracted from the encryption device in which information neither in the Plain Text form nor in cipher text form and between this duration encryption device produces easily measurable timing information, various types of radiation, power consumption statistics and many more information and hackers use some of or all of these information to get the key of IoT system. Fault analysis attacks, power analysis attacks, timing attacks and environmental attacks are some example of Side channel attack [9].

iii) *Cryptanalysis Attacks:* Encryption is the best way to secure any device or information, and in cryptanalysis attacks attackers try to break the encryption and try to get the encryption key, so that they can get the plain text from the cipher text. Middle-man-attack and close plaintext attack are example of this attack.

iv) *Software Attacks:*This type of attacks are the most common and most vulnerable attacks in any type of software. Attackers can easily spread up virus to any software that can damage all the system in few seconds. Trojan horse program, worms or viruses are the example of software attacks which intentionally inject malicious code into the system

v) *Network Attacks:*As we know that most of the IoT devices connected through unguided media which is more vulnerable to network security than guided media due broadcast nature of transmission medium. Network attacks are classified into two category i.e, Active attacks which includes DoS attack, Node malfunction, routing attacks, Node Capture attack, Node Outrage and Node subversion attack while on other hand Passive attack includes Monitor and Eavesdropping, traffic analysis, camouflage adversaries' attacks.

IV. ANALYSIS of IoT ATTACKS

IoT security is the main aim of the IoT device developers to provide a secure IoT environment to their users. Therefore, time-to-

 ISSN: 2454-4248
126 – 130

time many surveys are performed for IoT security form different perspectives.

In the field of IoT, there are many factors which affects the IoT security like, factors which make IoT security more challenging, factors that give security assurance and finally those factors which distinguish IoT security from traditional security. all these factors explored by Ray et al[1].

Study on trust management in an IoT environment is done by Guo et al [21] and Yan et al [10]. A research model based on trust management is proposed by Yan et al. [10] that based on the IoT system models. Trust management is not only the ensuring the trust management of each layer and cross layers but also ensuring the users about the security of IoT devices and services.

Characteristics of centralized and distributed system are studied in [11], that explains the challenges and promising measures which are involve in the deployment of distributed IoT security mechanisms, such as fault tolerance, trust, access control, authentication and protocols and network security.

Study of security and safety in IoT device is focused by Wolf and Serpanos[12] and Banerjee et al. [13]. Combination of Physical system with Network system has increased the chances of attacks on IoT. If any physical system is changed in an IoT environment, then all changes are also made in whole IoT system [12].

There are many IoT security solution issues which are most important to secure IoT environment, hence a survey is focused on IoT security solutions issues. A taxonomy that classifies the IoT security threats into four aspects is proposed by Alaba et al. [14]. these threats are related to data, application, architecture and communication. A research overview is also provided by [15], that shows efforts in terms of access control, authentication, privacy, authorization, middleware, confidentiality access control and trust in IoT.

Attacks on each layer of IoT three tier architecture is investigated by author in [15], and author also discuss the IoT security challenges. In [16], author consider all the techniques which are more or less security problem and in [17], author explain the different security issues which are belongs to the protocols and techniques which are concerning each layer of IoT environment and also introduced some solution to corresponding issues. They also explain the IoT security with regard to each layer of IoT system.

A) Security and IoT

Today, Security has prime role in each field of technology because without security everything is on risk and in the field for information technology where every information whether it is about living things or non-living things is available over the internet which is freely available to all without any constraints So this information can also be misused by any person from the entire world who can harm not only our equipment's but also our personal life. Security is a way that provides security, by security triangle, i.e Data Confidentiality, Data Integrity and Data Availability.

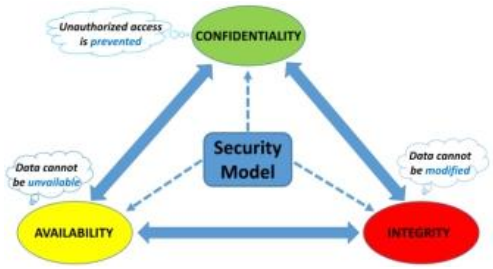

Fig 5: CIA Security Model

Data Confidentiality ensures the authentic user that his data/impersonal information keep in secret and only authentic person can accessed his information with his permission and an unauthorized person will not be allowed to use his information, generally this task is performed by encryption technic that converts the original text (plain text) into some other code (cipher text) by using a private key. many encryption techniques like RSA, DES, AES, DiffieHellmanetc. are used for encryption of data. Data confidentially can also be achieved by using access control mechanisms.

Data Integrity:Data / information generally hacked or steal during the transmission of data through guided or unguided media. during this transition of information hackers steal information and alter original information by adding or removing some information to original one.

Data availability ensures the immediate availability of original data to the user with free from any kind of alteration, It also prevent data from DoS(Denial of Service) attack and for this it uses firewall, IDS and redundancy methods.

B). IoT Security Requirements

Confidentiality, Authenticity, Integrity and Availability are the basic requirement for network security which must be followed by every device or service which are connected to internet [18], and same security measurement is allowed on IOT devices or services to protect data. Heterogeneity and constrained resources are two factors that always considered at the time of applying these on IoT architecture.

i) *Privacy:* the way of securing our data from an unauthorized user is referred as privacy, and in IoT it should be preserved because IoT devices collect the and involvement of human has increased the size of ubiquitous data that is the most important aspect. So privacy has become a prime aim of IoT ecosystem. Confidential data transmission ensures the privacy of data that secure the data fromattackers[19].

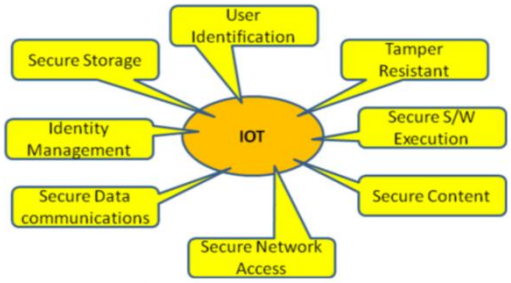

Fig. 7 IoT Security requirement

 ISSN: 2454-4248
126 – 130

ii) *Identity Management:* after increasing number of devices in the field of IOT, identifying the particular device has become more complicated because of complicated relationship among the users, services, devices and owners[20]. identity management is also a big challenge for secure IoT environment. For individual device, it is compulsory that it follow the rules for authentication, authorization with revocation and accountability or non-repudiation which are unique for each IoT device.

iii) *User Identification:* User Identification is the main step in IoT requirement that validate the authentic user for the use of system

iv)*Tamper Resistance:* Tampering with the devices is common problem in IoT system that is used by attackers to inject some malicious code or tempered the device by inserting some physical or logical probes. So, it is compulsory that all devices must have some tamper resistance that enable them to resist any kind of change.

vi) *Secure Execution Environment:* code that is going to be implemented in the system must be free from any kind of attack so that programmer can easily manage and protect code from malicious activities.

vi) *Secure Content:* Digital right Management (DRM) or content security is the best way to secure digital data that is used in the system.

vii) *Secure Network Access:* Network is the most important part in network transmission, if network is secure then information is also secure. So, a network access must be secured by some cryptography techniques so that only authorized person can get the access of network system.

viii)*Secure Data Communication:* Data is considered as the important part of any kind of information, if data is secure then information is secure and most of the data is hacked during the transmission of information, if we secure the data over communication then we can secure information. So we have to ensure the confidentiality and integrity of communicated data and also stop the repudiation of communicated in transaction.

ix) *Secure Storage:*IoT Data that is releasing over the internet must be secured at a secure place and that place must be authorized with some encryption techniques so that only few authentic persons can access that place. For example, if we are storing our data in a cloud then that cloud access must be secured by an authentic person

V. CONCLUSION and FUTURE WORK

After going through the critical review of security attacks on IoT system, it is well established fact that IoT systems are future of the communication technologies. However, IoT systems has some security loop holes that can breach the security of IoT system at any time, so it becomes most important that there must be some in-depth work in the field of IoT security that can secure IoTsystems data which is available over the internet, so that users can make themselves sure that they are using a secure medium to communicate with different physical devices and their data is in safe hands. And in future, some task like data security of IoT system and implementation of computational intelligence techniques like artificial neural network, Fuzzy System, Swarn intelligence and Evolutionary Computational can also be used to provide security to IoT systems.

REFERENCES

[1]. D. Giusto, A. Iera, G. Morabito, L. Atzori, The Internet of Things: 20th Tyrrhenian Workshop on Digital Communications, Springer Publishing Company, Incorporated, 2014.

[2]. M. Rouse, I. Wigmore, Internet of things, 2016. URL http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.

[3]. F.A. Alaba, M. Othman, I.A.T. Hashem, F. Alotaibi, Internet of things security: A survey, J. Netw. Comput. Appl. 88 (Suppl. C) (2017) 10–28. http://dx.doi.org/10.1016/j.jnca.2017.04.002

[4]. J. Granjal, E. Monteiro, J.S. Silva, Security for the internet of things: A Survey of existing protocols and open research issues, IEEE Commun. Surv. Tutor. 17 (3) (2015) 1294–1312. http://dx.doi.org/10.1109/COMST.2015.2388550

[5]. S. Sicari, A. Rizzardi, L. Grieco, A. Coen-Porisini, Security, privacy and trust in internet of things: The road ahead, Comput. Netw. 76 (Suppl. C) (2015) 146–164. http://dx.doi.org/10.1016/j.comnet.2014.11.008.

[6]. J. Zhou, Z. Cao, X. Dong, A.V. Vasilakos, Security and privacy for cloud-based IoT: Challenges, IEEE Commun. Mag. 55 (1) (2017) 26–33. http://dx.doi.org/10.1109/MCOM.2017.1600363CM.

[7]. Z.K. Zhang, M.C.Y. Cho, C.W. Wang, C.W. Hsu, C.K. Chen, S. Shieh, IoT security: Ongoing challenges and research opportunities, in: 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, 2014, pp. 230–234. http://dx.doi.org/10.1109/SOCA.2014.58

[8]. Sachin Babar1 , Antonietta Stango1 , Neeli Prasad1 , Jaydip Sen2 , Ramjee Prasad1,"Proposed Embedded Security Framework for Internet of Things (IoT)",

[9]. Hagai Bar-El ,"An Introduction to Side Channel Attacks " , White paper,Discretix Technologies limited,

[10]. Z.Yan, P.Zhang, A.V.Vasilakos, "A survey on trust management for internet of things", J.Netw. Comput.Appl.42(2014)120–134.

[11]. R.Roman, J.Zhou, J.Lopez, "On the features and challenges of security and privacy in distributed internet of things", Comput. Netw.57 (10) (2013) 2266–2279.

[12]. M.Wolf, D.Serpanos ,"Safety and security in cyber-physical systems and internet of things systems", Proc. IEEE 106(1) (2018) 9–20.

[13]. A.Banerjee, K.K.Venkatasubramanian, T.Mukherjee, S.K.S.Gupta, Ensuring safety, security, and sustainability of mission-critical cyber physical systems, Proc.IEEE 100(1) (2012) 283–299.

[14]. F.A.Alaba, M.Othman, I.A.T.Hashem, F.Alotaibi, "Internet of things security: a survey," J.Netw. Comput. Appl.88(2017) 10–28.

[15]. S.Sicari, A.Rizzardi, L.A.Grieco, A.Coen-Porisini, "Security, privacy and trust in internet of things: the road ahead", Comput. Netw. 76 (2015) 146–164.

[16]. Q.Jing, A.V.Vasilakos, J.Wan, J.Lu, D.Qiu, "Security of the internet of things: perspectives and challenges", Wireless Netw. 20(8) (2014) 2481–2501.

 ISSN: 2454-4248
126 – 130

[17]. Y.Yang, L.Wu, G.Yin, L.Li, H.Zhao, "A survey on security and privacy issues in internet of things", IEEE Internet Things J.4(5) (2017) 1250–1258.

[18]. Gunter Sch ¨ afer. ¨ Security in fixed and wireless networks - an introduction to securing data communications. Wiley, 2003.

[19]. JoergDaubert, Alexander Wiesmaier, and PanayotisKikiras. 2015 A view on privacy & trust in iot. In IOT/CPS-Security Workshop, IEEE International Conference on Communications, ICC 2015, London, GB, June 08-12, 2015, page to appear. IEEE

[20]. Srivaths Ravi, AnandRaghunathan, Paul Kocher, Sunil Hattangady ,"Security in embedded systems: Design challenges " ,August 2004 , Transactions on Embedded Computing Systems (TECS) , Volume 3 Issue 3 , ACM

[21]. J.Guo,I.Chen,J.J.P.Tsai,"A survey of trust computation models for service management in internet of things systems", Comput.Commun.97(2017)1–14.