International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 02 | Feb 2020 www.irjet.net p-ISSN: 2395-0072

A Study on Smart Way for Securing IoT Devices

Thrisha V.S[1], Dr.Anitha T.N[2]

[1]*M. Tech Student, Dept. of CS&E, S J C Institute of Technology, Chickballapur*
[2]*Professor & Head, Dept. of CS&E, S J C Institute of Technology, Chickballapur*

Abstract - *Usage of Internet has been widely increased in day-to-day life. Most of the human activities are done through internet in which the transfer of information from one place to another place is also done through internet. The information which we send from one device to another device is not been secured. To provide security to all IOT devices, functioning of security management should be done in a proper way. Currently security enabled model is developed to secure end-to-end communication in IOT environment. To overcome all these security problems in IOT devices a well secured solution is required. This paper deals with various different techniques which is used to secure IOT devices.*

Key Words: IoT, GSM, RPL, RFID.

1. INTRODUCTION

The amount of persons associated to internet is growing day-by-day and in the similar entity is also happening to all the strategies that are linked to internet to discuss the data and to cooperate with each other. Due to the massive increase in the population of the world, the usage of smart devices has also been increased. According to the current situation more than 100 countries are linked to exchange the data opinions through internet. This huge usage of internet by many people lead to a new problem called security. The safety administration of IoT policies is a chief problem which we are facing in now-a-days. Hackers can attack and get the information easily due to decrease in the security level of IoT devices.

IoT is a generous type of Worldwide System that is used to attach various things that comprises of smart machines, environmental objects and infrastructures and Radio Frequency Identification (RFID).

IoT devices are beneficial for many of the actual creation of applications and amenities and it can also be applied to build a small residence. In future, the major functioning of IoT is done through IoT. Wireless sensor networks, actuator networks and vehicular networks play a major role in the field of industry.

These devices has its applications in many areas like Industries, Educational Institutions, Hospitals etc. This mass usage of IoT devices in different areas leads to security problem where many techniques have been applied to collect, analyze and understand the problem.

1.1 Volume:

It is an extreme task in Bio-Diversity. The variety of such sort of material conservational information therapeutic information or data and commercial evidence. Facebook or Instagram, for example products of 500 terra bytes of data is utilized in each day and it is recognized from the description, the unpackaged counts. We cannot set any of the boundaries for the and it does not comprise any sort of data.

1.2 Velocity:

As it is stated in the previous filling to multiplicity and intricacy of the data structure, if more swiftness and large data is additionally joined, then the operation becomes a thought-provoking work. Speed is the another feature in which it is contested. The allowance of high-velocity figures is more stimulating.

2. RELATED WORKS

[1] Security Model for IoT based devices, in this paper writer advises a safety model in which the IoT supports the characteristics for protecting the data from unauthorized access. Initially perception layer is the main source for collection of data and all the real time data is thus collected by Radio Frequency Identification Devices(RFID) and each layer of IoT structure face challenges for providing security and privacy. In this security model we also have a massive foundation of fog computing and storage which helps in managing the administration of fog objects.

[2] A survey on IoT security challenges, in this paper author propose challenges for random access mechanisms to protect IoT devices. The two mainly used mechanisms are overlapped contention and segmented contention. The overlapped contention contains two layers upper bound and the lower bound in which windows can share all the nodes in zero level which is determined as lower bound. In segmented contention, Upper bound is the better way to share all the nodes. The proposed mechanisms are analyzed, implemented and evaluated on linux based testing and NS3 simulator.

[3] Security on IoT and its smart Appliances, in this paper author proposes an idea to provide security for smart appliances. This can be achieved when the appliances are connected to MCU/embedded system processor with an unique ID. Global System for Mobile Communication (GSM) is also provided to control message or information displayed without showing the location of the user. Further open

wireless skill such as Bluetooth, Wi-Fi and also the telephonic information facilities and also embedded sensor and actuator nodes are made to use in keen appliances.

[4] Ongoing challenges and research opportunities, in this paper author proposes different challenges and opportunities given to secure IoT devices in which one of the important challenge is technology challenge. By using advanced technology many people hack the devices to get information which is kept confidentially and hacking process has become common in many of the private companies and government agencies. Therefore security should be increased in these fields to avoid hackers and apart from these Artificial intelligence, security and privacy are the new challenging aspects of IoT devices. Research opportunities are provided to improve connectivity, architecture and robustness in all IoT devices.

[5] Effect of IoT new features on security and privacy , in this paper author proposes newly introduced features on security and privacy which developed a great effect on IoT devices. Intrusion Detection system(IDS) and Intrusion Prevention System (IPS) models are used to defend dissimilar kinds of campaigns at the similar time that are mostly based on heterogeneous IoT devices and these are mainly used in the detection of traffic network. If IoT devices are light-weight in size then they will not have memory management unit(MMU), so Memory Isolation Address Space Layout Randomization (ASLR) and other security actions cannot be unswervingly deployed on these diplomacies. It is a tough mission for the researches to deploy much multifaceted encryption and authentication algorithms on minute IoT devices.

[6] Security analysis of Big Data on IoT, in this paper writer suggests the working of safety and communication in IoT by using Big Data which contains high volumes of data. The information system which is based on IoT initially collects the information from the sensors, RFIDs and other smart devices to store them in the memory and get processed in the servers with high ultra strength and power. Google and Amazon companies support these powerful servers. The important analysis done between IoT and Big Data is congregation the environmental data, GIS and stargazing through the wireless sensors of IoT policies.

[7] Security Issues in IoT, in this paper author proposes a mechanism to protect personal information. Personal Medical Devices(PMDs) are used to know the present condition of the patient. These PMDs contains wireless interface which is used for communication purposes and to read status of the device, medical reports and also to update the status. Personal information can also be stored in smart homes where all smart devices are connected to internet environment and then smart home services contains digital services which can efficiently communicate with each other by using Internet Protocol(IP) addresses.

[8] A Review on Security in IoT, in this paper author proposes different layers in which all IoT device scan be secured. The basic layer is the perception layer(recognition layer) which is used to recognize the security problem in a particular device which helps to collect all types of information by using physical equipment which includes RFID reader, different sensors GPS etc. The transmission of information, classification, processing is done through network layer. For improving the ability to recognize the problem support layer is used. Data sharing is one of the most important aspect in application layer and ton solve the protection problem in application layer authentication and privacy protection is used where Advanced Encryption Standard(AES) algorithm is used to maintain confidentiality.

[9] A Survey of Security challenges in IoT, in this paper author proposes about the incompatibility which is a original contest facing aspects of IoT distressing numerous zones mainly in the field of security where Privacy Enhancing Technologies(PET) is developed to attain confidentiality areas which include Virtual Private Networks(VPN) Transport Layer Security (TLS) and Peer-to –Peer (P2P) . In Order to investigate the safety problems in a better way, IoT is divided into different layers such as devices, Gateways, and applications/services. A usual group of sensors form the network named as “Sensor Network” which helps in the interaction of devices and Internet Protocol(IP) is used in a wider range for addressing in IoT.

[10] Design Challenges on Security of IoT systems, in this paper author proposes Computer Aided Design(CAD) technique to provide security for IoT devices in which CAD variable is present for optimization of schemes with a huge quantity of powerfully cooperating machineries and this sort of functioning occurs internally in many of the significant evolving schemes such as information centers and podiums. The main aim is to provide hardware based security which is suitable to answer all the requirements of IoT security and also to provide efficient solutions to solve many unsolved problems of cryptography in which one of the problem is security problem.

Table -1: COMPARISON OF DIFFERENT TECHNOLOGIES

SL No	Technology	Advantage	Disadvantage
1	RFID	High level security, quick response	Cost effective, low range coverage
2	NS3 Simulator	Improves the network performance	Problem occurs due to large scale devices
3	Embedded processor, GSM	Open source, queries are answered quickly	High cost, requires more staff
4	Artificial Intelligence	Efficiency is improved, low	Storage is expensive

		error rate	
5	IDS,IPS	High level protection	Low latency
6	Big Data	High volumes of information is stored	Light-Weight devices are not processed
7	PMD,IP	Data authentication, end-to-end protection	Loss of services, physical security risk
8	RFID,GPS	High security, easy installation	Low speed
9	Network sensors	Organizing capability, high scalability	Risk in securing Wi-Fi network
10	Ultrasonic sensors	Can sense all materials	Highly sensitive to external environment

3. CONCLUSION

In this paper we have discussed different techniques to secure IoT devices. The best and shortest solution which we have obtained to solve the problem of security in IoT devices is providing security enabled model to secure end-to-end communication in IoT environment. Apart from this various solutions have been provided to solve different security issues.

REFERENCES

1. Z. Safdar, S. Farid, M. Pasha, K. Safdar, " A Security Model for IoT based Systems" in Technical Journal , University of Engineering and Technology (UET) Taxila , Pakistan vol.22 No. 4-2017 ISSN:1813 - 1786 (print) 2313 -7770 (online)
2. Shubhalika Dihulia , Tanveer Farooqui , " A Survey on IoT Security Challenges " in International Journal of /.mputer Appliances (0975-8887) volume 169 – No.4, July 2017
3. Vandana Sharma , Ravi Tiwari " Security on IoT and its Smart Appliances " in International Journal of Science , Engineering and Technology Research (IJSETR), volume 5, Issue 2, February 2016
4. Sachin Upadhyay "Ongoing Challenges and Research Opportunities " in International Journal of Engineering Technologies and Management Research,5(2:SE),216-222 . DOL:10.6281/Zenodo.1195065
5. Wei Zhou , Yuqing Zhang , Peng Liu "Effect of IoT new features on security and privacy " in The College of Information Sciences and Tcehnology, The Pennsylvania State University , PA 16802,USA
6. Saeed Banaeian Far , Azadeh Imani Rad "Security analysis of Big Data on IoT " in IEEE transactions in Industrial informatics 12.3(2016): 1232-1242
7. Mirza Abdur Razzaq , Muhammad Ali Qureshi , Sajid Habib Gill , Saleem Ullah "Security Issues in IoT " in (IJASCA) International Journal of Advanced Computer Science and Appliances , volume 8, No.6,2017
8. Hui Suo , Jiafu Wan , Caifeng Zou , Jianqi Liu "A Review on Security in IoT " in 2012 Intenational Conference on Computer Science and Electronics Engineering
   Anass Sedrati , Abdellatif Mezrioui "A Survey of Security Challenges in IoT " in Advances in Science , Technology and Engineering Systems Journal volume 3 , No 1,274-280(2018)
10. Teng Xu , James B Wendt , Miodrag Potkonjak "Design Challenges on Security of IoT Sytems " in IEEE Journal on Selected Areas in Communications , volume 24, No 2,381-394(2014)