International Journal of Research in Advent Technology, Vol.7, No.6S, June 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

Estimating Security in the Internet of Things

Jeevan M., Gnana Sudha T., Shreehari B.V., Manjunath S., Vikas Reddy S.

Abstract— Growing number of IoT devices has led to issues regarding security and privacy. IoT security is happening to be at its crucial stage. So, we have come up with this survey wherein we have tallied a pile of papers that give various technological implementations and proposals as to how security challenge can be tackled upon. In this paper, we discuss briefly about the merits and demerits of the papers surveyed. By picking up the best implementation or idea proposed, we draw a conclusion to this survey.

IndexTerms— IoT, IoT security, privacy.

I. INTRODUCTION

IoT– the Internet of Things! "Things" here refer to devices and hardware that are 'connected'. Internet is network of the networks; and network in turn is connecting. With the increasing advancements in technology out there, IoT has been topping the hit list. Is that because it's new? No! It has been the best advancement that gets together all the devices that are allowed to share the same network access, hardware devices, and the Internet above all. Lots and lots of IoT devices are coming into existence. As a matter of fact, IoT is finding its way in through all the fields of improvement needed throughout the globe. A rough estimation of 50 billion IoT devices are expected by 2020.

When we figure out that a pretty huge number of IoT devices are showing up, there's a transpiration of security and privacy matters. The large number of devices interconnected deal with an entirely heterogeneous technologies and topologies. One cannot be given an assurance of a hack – proof connection with such diverse parameters. Once we realize that the network is poorly connected, we begin to worry about data protection. We wouldn't even choose to be in a network that doesn't respect privacy of one's information. In this paper, we have made a detailed survey on a bunch of papers that talk about security of IoT system.

II. LITERATURE SURVEY

IoT is connecting the unconnected. While connecting devices worldwide, two major factors that pops up are security and privacy. Consumers wouldn't know how secure their device is. If manufacturers produced devices with Consumer Security Index (CSI) [1], consumers readily purchase such devices. A study on the value of security label depicts how many customers prioritize security. Consumer's reliability on the security label completely depends on how he/she has presumed it to be.

Lot of surveys say that by 2020, 20 – 50 billion devices would be connected. With a large number of devices interconnected, security issues are more prone to arise in the near future. In such scenarios, security functions can be framed and manipulated considering the requirements accordingly. On – demand security configuration [2] simply deals with checking out how security works on the device, determine required functions, and reboot the device to enable security functions.

The IOT is predominantly being deployed in every part of the world; leaving behind security, which is definitely a biggest threat if misdealt with. Manifestation of security here is concerned to all aspects. The Information Security Sharing System [3] allows one to collect, store/retrieve and link information based on relevance to any fraudulence. The reference model has these processes: Collecting would refer to piling up that information which seem scrupulous; Verification and analysis meant validating information if it weren't malignant; Sharinginformation in the most righteous way.

Today, the field of smart devices is booming. A smart home system [4] in IoT environment, brings the organisation of home, to the fingertips of user. But, the major challenge here is the security. The intensity and the type of security required, vary with devices and services. In this system, we have a home server, that stores all the information, a home gateway takes care of the internet connection and the smart devices provides the service. For enhanced security, the data is to be converted to cipher text before transferring. Device identification system has to be developed such that no outsider shall communicate to the system, using a replica of my device. Passwords must be very strong (especially at the gateway) and have to be changed often. An algorithm, more secure than 128 bit encryption is adviced for use. Reciprocal authentication is to be established in the system. Abnormal operations of the devices have to be noted. A system to locate the device physically has to be established. Any external attack towards the system should be detected. Provided all such security facilities, the Smart Homes can be operated with no worries!

Blockchain is the most happening technology. The technologies connected to each other over the Internet can be reconsidered for modifications using the Blockchain technology. The 4 major pillars of Blockchain are: Consensus – it lays out the proof – of – work (PoW); Ledger – has all the details regarding the transactions in the network; Cryptography – all data in Ledger should be encrypted and

Manuscript revised May 13, 2019 and published on June 5, 2019
Jeevan M., *Student, Dept. of CSE, S J C Institute of Technology, Chickballapur.*
Gnana Sudha T., *Student, Dept. of CSE, S J C Institute of Technology, Chickballapur.*
Shreehari B.V., *Student, Dept. of CSE, S J C Institute of Technology, Chickballapur.*
Manjunath S., *Assistance Professor, Dept. of CSE, S J C Institute of Technology, Chickballapur.*
Vikas Reddy S. *Assistance Professor, Dept. of CSE, S J C Institute of Technology, Chickballapur.*

doi: 10.32622/ijrat.76S201917

can be decrypted only after authorization; Smart contract – V&V on all participants on network [5]. Altogether, its pretty difficult for Blockchain technology to meet the high – end requirements of security of the Internet of Things technology.

Automobiles aren't just a show case of status these days, it's become a major part of one's life. With increase in sale of automobiles, the number of accidents are also hiking on a larger rate every hour. To circumvent these accidents, inclusion of an intelligent integrated system [6] in the automobile is done. It is embedded with parameters like temperature, humidity, oxygen content, and Wi-Fi module. When people are left alone in the vehicle, the embedded intelligent life monitoring system sends alarm stating the parametric condition of the person locked up inside.

Authentication is verification of a user that wants to communicate with another one. To achieve this, we can make use of biometrics like fingerprints, DNA, retina, iris, face and other authentication mechanisms. Message authentication deals with encryption and decryption algorithms. Physical Unclonable Function [7], or PUF, takes a challenge as an input and produces out a response. A PUF based Authentication Scheme, or PAS, can be used for registering smart devices of a smart home. If any biometric parameter isn't registered, the gateway simply saves it, inputs it as a challenge so as to derive at a valid response. Evaluation of the controlled PUF with an improvised security is still a challenge.

The remote security management server [8] can be made use of to improvise on the security of IoT devices. This server has a handful of functions that are an integral part of the system, working on the security of the IoT devices. Hackers don't look out for networks in the recent times, instead, IoT devices are the ones they look out for. The remote security management server's job is to make sure that IoT devices aren't the hackers' tool anymore. It provides the next level security and privacy of information. Existing security functions are hardly utilized, so the RSMS plays as a substitute for security.

Wireless Sensor Networks [9] uses a number of sensor nodes belonging to various types. It is used for localization of objects. Each sensor in the network collect data and transfer it to all other sensor nodes in the network. WSN helps in long distance data transmission. Internet of Things, here, provides Internet to all the sensor nodes within the network. Real Time Locating System is used for locating objects, people or assets. Exposure to newest and the most efficient strategies for location tracking is being talked about.

A low cost technology for controlling and predicting condition of internal hardware can be implemented in connected vehicles. A cloud based system [10] is used for capturing live vehicle diagnostics. Machine learning based algorithm is used for prediction. Speed sensor, Pressure sensor, Vibration sensor, Temperature sensor, CO_2 emission sensor, GPS coordinates sensor and a fuel level indicator sensor are the list of sensors that shall be considered while implementing. All information collected will be transferred to a mobile application using WiFi gateway and cloud database.

III. CONCLUSION

While sharing intimate information, authentication and authorization of network, information and end users should be taken into consideration. To ensure the security based on Internet of Things, we would like to wind up this survey stating that security wouldn't be an issue if functions contain light – weight (less memory, fast processing) algorithms and techniques. Be it any system discussed above, if implemented using a light – weight algorithm, security and privacy are respected.

REFERENCES

[1] J M Blythe, S D Johnson, "The Consumer Security Index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices"
[2] Boheung Chung, Jeongyeo Kim, and YoungsungJeon, "On-demand security configuration for IoT devices"
[3] Jongsoek Choi, Yongtae Shin,andSunok Cho, "Study on Information Security Sharing System among the Industrial IoT Service and Product Provider"
[4] Boheung Chung, Jeongyeo Kim, and YoungsungJeon, "On-demand security configuration for IoT devices"
[5] Madhusudan Singh, Abhiraj Singh, and Shiho Kim, "Blockchain: A Game Changer for Securing IoT Data"
[6] Fei Ni, Jianxiang Wei,andJianhuaShen, "An Internet of Things (IoTs) based Intelligent LifeMonitoring System for Vehicles"
[7] Muhammad Arif Mughal, XiongLuo, ZahidMahmoodand Ata Ullah, "Physical Unclonable Function Based Authentication Scheme for Smart Devices in Internet of Things"
[8] Seungyong Yoon and Jeongnyeo Kim, "Remote Security Management Server for IoT Devices"
[9] Prof.Shital D. Bachpalle and Prof.Minakshi R. Shinde, "Integration of Sensors for Location Tracking using Internet of Things"
[10] Ashwin Srinivasan, "IoT Cloud Based Real Time Automobile Monitoring System"

doi: 10.32622/ijrat.76S201917