Security in the usage of IoT devices

Nikila GS, Rishab GSS ,
Computer Science Engineering, Mechanical Engineering,
Vellore Institute of Technology, Vellore, India.

Abstract— In our day to day life we come across many implementations of IoT devices. Such devices indeed do make life easier. But these devices come with a certain amount of technical drawbacks. It is not easy to protect such devices from being hacked as we know they can be very easily hacked with the right mechanism. Even though IoT devices offer us a simple life, they do not always promise us security that the user expects. There have been many researches that have taken place from the years 2016 to 2019 to increase the user security and this paper gives another such solution to secure the devices of IoT. Here we will discuss the key technologies used such as encryption mechanisms, cryptographic algorithms, protecting sensor data and communication security.

Index Terms—Internet of Things; Privacy; Security; Cloud computing ; Device FingerPrint; Discretion; Challenges .

1 INTRODUCTION

The Internet of things is a well known concept in the current world and many concepts of IoT are being implemented every day. There are new concepts arising and equally new threats that degrade the security offered by these devices. Personal data of the users are stored in these devices and these devices are linked to each other through the Internet. As the number of devices and sensors that are connected to one network increases, the security of the devices compromises with the number of devices. This is a huge drawback in the advancement of the devices of IoT. Numerous researches have been carried out to solve this problem and many prominent ones are being used with modern devices. IoT is gaining momentum in the horizontal and the vertical markets and these devices have the ability to change the routine of a normal human. For instance let's take an example, Suppose you are on your way back home in your smart car, the car is capable of communicating with other cars to avoid accidents and if you want to take a hot shower once you get home, you could just use voice command in your car to switch on the heater back home. Over here, the car and the heater are connected to one another through a set of sensors which are in turn connected to the internet. We live in a world in which devices of every shape and size are manufactured with smart capabilities that enable these devices to communicate with humans, exchange data with one another, make autonomous decisions and perform tasks based on the environment.

Before the emergence of IoT, we had Machine to Machine (M2M) communications. The machines are the end points and they are capable of communicating with each other without human interference. This trend is still in use in many fields. Over the past decade, the field of IoT has immensely improved on various factors and now ranges to a huge variety of utilization. It is being used in e-commerce, e-healthcare, traffic monitoring systems, home automation systems, air pollution monitoring systems, etc. With the rise in advent of this industry, it is predicted to reach up to 50 million connected devices by the year 2020. But the horrors of these delicate devices being hacked still remains to scare the population. The solution for this is being developed and improvised everyday to secure the information that is crucial to the users or the population.

2. EMBEDDED SYSTEMS

An embedded system is a microprocessor or a microcontroller based system which connects software and hardware components to perform a set of dedicated functions. The software that is designed to perform a dedicated function, either as an independent system or as a part of a large system. At the core is an integrated circuit designed to carry out computation for real-time operations.

The complexity of an embedded system ranges significantly. It ranges from a single microcontroller to a suite of processors with connected peripherals and networks. The complexity of the embedded system differs depending on the task for which it is designed.

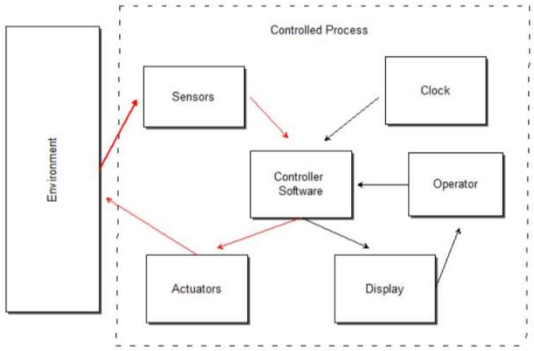

Fig. 1: controlled process.

Embedded systems have a lot of applications in our day to day lives, starting from our toasters to helicopters. Almost ninety eight percent of the manufactured microprocessors are used in embedded systems. It is because of their large applicability and convenience embedded systems are found everywhere in our day to day lives. This piece of technology has improved life on a large scale.

Microcontrollers or microprocessors control the entire functioning of the embedded systems. They are also controlled by digital signal processors(DSP) or application specific integrated circuits(ASIC), field programmable(FPGA), GPU technology and gate arrays. These processing systems are integrated with components dedicated to handling electric and/or mechanical interfacing.

The instructions to these embedded systems are stored in a read only flash memory chip, running with limited computer hardware resources. Peripherals are used by the embedded systems to connect with the outside world by linking input and output devices.

BASIC STRUCTURE OF EMBEDDED SYSTEMS

1. Sensor: a sensor is used to convert a physical quantity into an electrical signal, which is either read by an electronic instrument or an embedded systems engineer. A sensor is used to store the measured quantity to the memory.
2. A-D Converter: an analog to digital convertor converts the analog signal sent by the sensor into a digital signal.
3. Processors: the output is assessed by the processor and is measured and stored in the memory.
4. D-A converter: a digital to analog convertor converts the digital data fed by the processor to analog data.
5. Actuator: the comparison between the output given by the D-A converter to the actual output stored is done by the actuator. The actuator after comparison stores the approved output.

3. LITERATURE REVIEW

The Internet of Things (IoT) bolsters a wide scope of uses including keen urban communities, traffic blockage, squander the board, auxiliary wellbeing, security, crisis administrations, coordinations, retails, mechanical control, and social insurance. IoT is megatechnology that can build up association with anything, anybody, whenever, place, administration on a stage and any system. It greatly affects the entire square chain of organizations, keen articles and gadgets, frameworks and administrations that are empowered by heterogeneous system availability and is created as a brilliant unavoidable structure of savvy gadgets. IoT gadgets are being used in numerous fields, they associate with complex gadgets, interface with antagonistic conditions and are sent on different uncontrolled stages, accordingly faces numerous security issues and difficulties. Since the IoT offers a potential stage for coordinating any sort of system and complex framework it could experience vulnerabilities characteristic to the individual frameworks which are accessible inside the incorporated system. This paper is an investigation of the security issues of the individual frameworks answerable for IoT interconnection and their effect towards the coordinated IoT framework.

4. SECURITY

The biggest disadvantage of IoT devices is it's security options. As the number of IoT connected devices continues to increase in the following years, so will the number of malware and ransomware used to exploit them. Previously this issue was because of the fact that manufactures did not care much about securing their devices properly but then after the rise of hackers and the realization of privacy breach they brought upon new version of security patches and fixes but hackers could still easily pass through older software versions of the IoT device this was because the users did not tend to update their device that would have led to increase in its security. Hence it is crucial to set up an efficient system that would have a simple yet effective way of securing such devices.

Even though the blockchain is highly resistant to hacking, the number of attacks in these sectors is increasing as technology rapidly advances. Social engineering is already being used as a key tool to extract usernames, passwords and other private keys ranging from social media accounts all the way to bank account details and we can notice it being more often in the future to hack blockchain-based apps. Every poorly connected device in the internet means that it is a potential threat to the security of the devices on the internet. This to be secured safely so that there are no outbreaks in the privacy of the user.

In order to do this, we have proposed a method using which only the authenticated user using a specific device will be able to control the other devices that are connected in the circuit.

IoT is wonderful in many ways, but sadly technology has not developed enough and it is not completely safe to use these devices. The entire environment of IoT has many challenges to overcome and hopefully these challenges will be overcome in the near future.Lack of user knowledge and awareness is one of the major reasons that degrade the security factor of IoT devices, so users must be educated about these devices before they can be put to use.

5. DEVICE FINGERPRINT

This is a technique put forth to secure the privacy of the user such that no hacker will be able to obtain the delicate information from the devices without the user's permission. This can be done with the help of a set of numbers that are particularly unique to the device. Some of the numbers that are being used in this paper are

1. Model number
2. IMEI number
3. Build number
4. IP address
5. Phone Number

These numbers are randomly selected and are unique for every different device and are finally stored in the cloud. Since the numbers are randomly selected it will be extremely challenging for the hacker to find the correct set of numbers to hack the devices of the Internet. The numbers that are selected are encoded using the XOR operation to give a final unique value. This value is hence called as the device fingerprint.

Since IoT devices are frequently prone to attacks and are not legitimately secure as we think they are, this system in place will be an effective security measure that will drastically protect the integrity of these devices. From Fig.1 below it is seen that the hacker can access the information and alter the instructions sent by the user very easily. In order to avoid such unfortunate circumstances we select a set of device specific numbers. The cloud will accept and store the data given by the device if and only if the device fingerprint matches with the pre existing device fingerprint value.

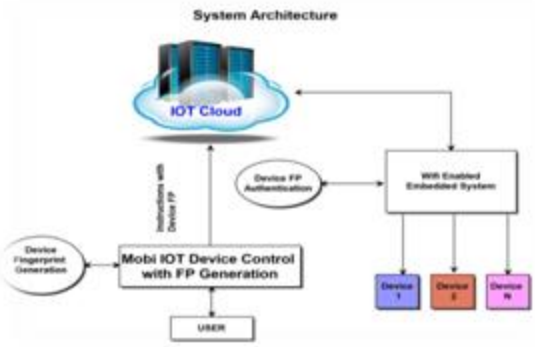

Fig 2: diagrammatic representation of the architecture.

Using such a number makes sure that there are a numerous numbers of permutations and combinations so as to detect which device specific number is being used. This causes ambiguity for the hacker and minimizes the chances of the device being used by an unauthorized person or device.

The system architecture is denoted in Fig.1 from this it is seen that the device fingerprint is generated with the help of Mobi IOT Device Control by the user. This data is stored in the IOT cloud. This is the region where the hacker could try and access the code. But with the help of Device Finger print this process would be quite tedious and in most cases impossible. The data that is being stored in the cloud is then used by the WiFi Embedded System. This system could be either an arduino board or a raspberry Pi. The Device fingerprint is authenticated here. If it is done successfully the command to the devices are given, that is, the information store in the cloud is successfully transferred and executed.

The table 1 below gives how a device fingerprint is generated from the taken set of numbers. It is essential to keep in mind the order of the numbers taken and to remember that this number is only device specific and not confined to the individual.

Table 1.

HEX numbers	XORed HEX numbers
10073107237	86D79F0175B4A7A
9008311777	
867287036425721	
a501043191008	
19216813	

Further security can be provided for these devices by keeping a user specific password which enables only that particular user to perform a specific function. The integrity of the device is secured by doing so. This technique reduces the risk of an unknown body accessing the details that are to be protected.

6. CONCLUSION

In the past few years there has been a surplus of technology and these technological advances require adequate security measures. Researchers have been trying to cope with this to deliver the accurate protection to the devices and the content within each of the devices. In this paper we present to you an idea to find a device specific unique number which secures the connected smart devices. The cloud architecture is represented in the diagram and an example for how this algorithm works is also presented in this paper. From this it is clear that only a specific device will be able to operate on this and enable the functioning of the other connected devices.

7. REFERENCE

[1] Suo, Hui & Wan, Jiafu & Zou, Caifeng & Liu, Jianqi. (2012). Security in the Internet of Things: A Review. Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012. 3. 10.1109/ICCSEE.2012.373.

[2] M. H. Miraz, M. Ali, P. S. Excell and R. Picking, "A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT)," 2015 Internet Technologies and Applications (ITA), Wrexham, 2015, pp. 219-224.

[3] Y. Chahid, M. Benabdellah and A. Azizi, "Internet of things security," 2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS), Fez, 2017, pp. 1-6.

[4] Elisa Bertino, Kim-Kwang Raymond Choo, Dimitrios Georgakopolous, and Surya Nepal. 2016. Internet of Things (IoT): Smart and Secure Service Delivery. ACM Trans. Internet Technol. 16, 4, Article 22 (December 2016), 7 pages.

[5] Abid Sultan, Muhammad Azhar Mushtaq, and Muhammad Abubakar. 2019. IOT Security Issues Via Blockchain: A Review Paper. In Proceedings of the 2019 International Conference on Blockchain Technology (ICBCT 2019). Association for Computing Machinery, New York, NY, USA, 60–65.

[6] Francesco Buccafurri, Gianluca Lax, Serena Nicolazzo, and Antonino Nocera. 2017. Overcoming Limits of Blockchain for IoT Applications. In Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES '17). Association for Computing Machinery, New York, NY, USA, Article 26, 1–6.

[7] M. Abomhara and G. M. Koien, "Security and privacy in the Internet of Things: Current status and open issues," in Int'l Conference on Privacy and Security in Mobile Systems (PRISMS), 1-8, 2014.

[8] K. Zhao and L. Ge, "A survey on the internet of things security," in Int'l Conf. on Computational Intelligence and Security (CIS), 663-667, 2013.

[9] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization," Computer Networks, vol. 56, 3594-3608, 2012.

[10] M. Leo, F. Battisti, M. Carli, and A. Neri, "A federated architecture approach for Internet of Things security," in Euro Med Telco Conference (EMTC), 1-5, 2014.

[11] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (iacac) for the internet of things," J. of Cyber Security and Mobility, vol. 1, 309-348, 2013.

[12] M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," Perception, vol. 111, 2015.

[13] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things,"Computer, vol. 44, 51-58, 2011.

[14] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, 2266-2279, 2013.

[15] Q. Wen, X. Dong, and R. Zhang, "Application of dynamic variable cipher security certificate in internet of things," in Int'l Conference on Cloud Computing and Intelligent Systems (CCIS), 1062-1066, 2012.

[16] G. Zhao, X. Si, J. Wang, X. Long, and T. Hu, "A novel mutual authentication scheme for Internet of Things," in Int'l Conference on Modelling, Identification and Control (ICMIC), 563-566, 2011.