Analysis of Hardware and Software Security Challenges in IoT

[1]Pooja V. Chavan, [2]Prof. Mansi Kambli
[1]M.Tech Student, [2]Professor
Department of Computer Engineering,
K.J.Somaiya College of Engineering, Mumbai, Maharashtra, India
Email:*poojachavan8111@gmail.com*

DOI: *http://doi.org/10.5281/zenodo.2267384*

Abstract

Internet of things is an emerging trend that developed many technologies, where each and every device connected through network and can be controlled from remote location. IoT is a successful beneficial technology. It is a backbone for smart home, smart City, e-agriculture, smart grids, smart farming. There is lots of security and privacy flaws occur in IoT enabled device especially for software, hardware and hybrid prospective. IoT network security and privacy are very important aspects for application domain. To get complete secure environment by using protocols, methods, IoT security framework, security and privacy policies and security algorithm. The main objective is to develop a secure IoT technology. "Without trust and security, Web services are dead on arrival".

Keywords:*IoT, Web services, digital, technology*

INTRODUCTION

We all are living in digital world, everything is being connected through internet. IoT is going to be an inevitable part of our daily lives. 'Internet' and 'Things' are two very important aspects. IoT requires such a network that available anytime, anywhere and things are nothing but sensors, actuators and RFID tag element. Internet of Things is a successful technology; it helps companies to deliver great customer services to develop new business models.

There are lots of security and privacy challenges facing by internet of things. The basic fundamental security models are confidentiality, availability and integrity. Using CAI and security algorithm we can protect components of IoT system. IoT device have some vulnerabilities such as loss of confidentiality, integrity and availability. Now a day's adoption rate of IoT device is very high, more and more devices are to be connected through internet. In that major security and privacy flaws in IoT enabled device especially from hardware and software perspective. In a network there are huge number of objects are connected to each other. It's very difficult not only to manage huge information of objects but also to secure them. Providing a security for IoT environment is very challenging task. Security and privacy threats are not bounded only software level it's also occur in a hardware level. Security issues are increasing day by day it's not good for developer as well as researcher.

NEED FOR SECURITY IN IOT

IoT plays important role in healthcare monitoring. Implementation of healthcare for heart rate based on IoT devices, including patients' information, medical doctor, this system beneficial for hospitals example, healthcare system in heartbeat rate monitor by smartphone and if there is something wrong it will call the nearest hospital for ambulance. The smartphone will send person's current location to the nearest hospital, they will extract the location and pick that person to hospital after that doctor will start the treatment on that person. It sounds great, but if the IoT based system is not secured it may cause death of person. Example home, let us consider a smart security system inbuilt in home for security. Imagine, we install camera everywhere. If someone hacks that security system and get control on camera, worst scenario. It's very clear without security and privacy IoT could be a worst rival for our daily lives.

CHALLENGES IN IOT

The IoT devices are distributed systems, clients predicted the system to be secure and reliable. The challenges including availability, confidentiality, authentication, authorisation, gateway security and so on.

1. IoT device are too small in size, it's very difficult to add extra security model in small things.
2. The security complex algorithm is used in IoT device but most of the IoT devices have low computational capabilities, so the complex security algorithm is not suitable for small IoT devices.
3. The small IoTdevice has limited power and it's a barrier to security. Software and hardware require endless power to add extra security which is required in module, and also need an energy to perform. The IoT system is always work on energy efficient.
4. The hardware based device are insecure after the few days, we cannot add extra module to perform better result because updated hardware module is not immediately integrated.
5. The software based things become outdated after the few days because we cannot update immediately, it requires work on lots of phases and each phase is dependent on each other.
6. The physical layer is not used in industry because lots of security issue occur till now. The electronic device is facing a hardware issues which are increasing day by day.

SECURITY ISSUES LEVEL

This security issue broadly categorised in three sections: Hardware level security issues, Software level security issues, and Hybrid level security issues.

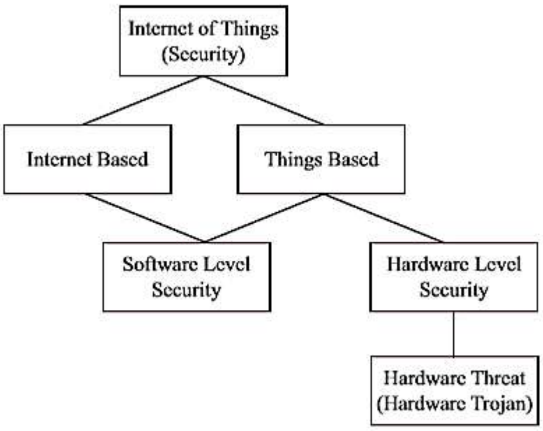


Fig: 1.*Software and Hardware level security in IoT*

HARDWARE LEVEL SECURITY ISSUES

Hardware level security issues are growing day by day. The researcher pay attention on insecurity like authentication, access control, client privacy and other attacks. IoT system requires complete hardware security, we need to secure the IC from network on chip and system on chip. VLSI in design and fabrication are the two different things which are completely work on distributed system. The selection of fabrication process depends on vendor because integrated circuit is very costly. In a design phase, we can inject a single malicious circuit. Threads can be injected any phases of life cycle, but integrated circuit is a successful fabrication. If a thread is injected in a hardware system then we can loss aconfidential information. Hardware Trojan is one of them.

Example,Raspberry Piis a famous hardware component in IoT. It’s a single board computer. Linux.muldrop.14 is one type of Trojan that occurs in a Raspberry Pi. The Linux.muldrop.14 Trojan is basically described as a Bash script. Bash script is a one type of file in DOS. This Trojan specifically target Raspberry Pi. Once the Trojan is inserted in a Raspberry Pi it will automatically change the system password. Linux.muldrop.14 solution is wipe out the SD card and reinstall the operating system otherwise stop all the system resources.

SOFTWARE LEVEL SECURITY ISSUES

Software level security issues are hacking, authentication, authorisation, information leakage, integrity availability etc. Daily lives we use high-tech system but that system should have security and privacy protection if security is not available then we cannot use to dare that systems. It is possible, unauthorised user can enter into the system and access the personal information or credit card information.

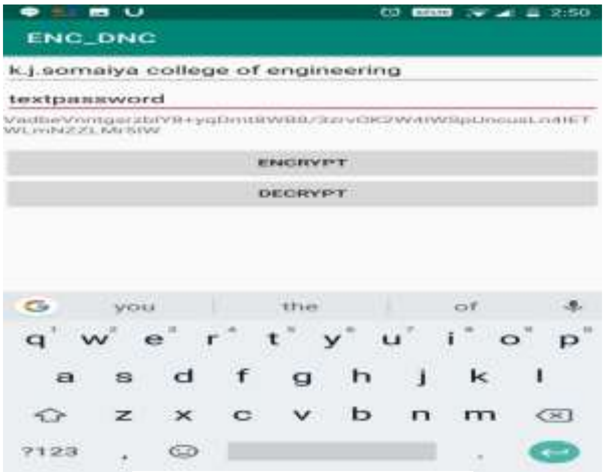
Software Components Based Technology in IOT

Near Field Communication (NFC)

NFC is a short range wireless technology. It's an allowing communication between two devices with 13.56 MHz’s. When two devices are communicating with each other using NFC technology they require some communication protocol like core protocol, peer to peer protocol, EVM (European MasterCard visa). Near field communication in transferring data rate is very high and require less energy and easy to use. NFC chip is work on antenna. The inbuilt location of antenna depends on the mobile phone. Near field communication use for data transformation. We can secure that communication data with the help AES Algorithm. It is energy efficient and less complex that why used in NFC to secure the information.

Android Application

Implementation of Android Application for encryption-decryption message using AES Algorithm

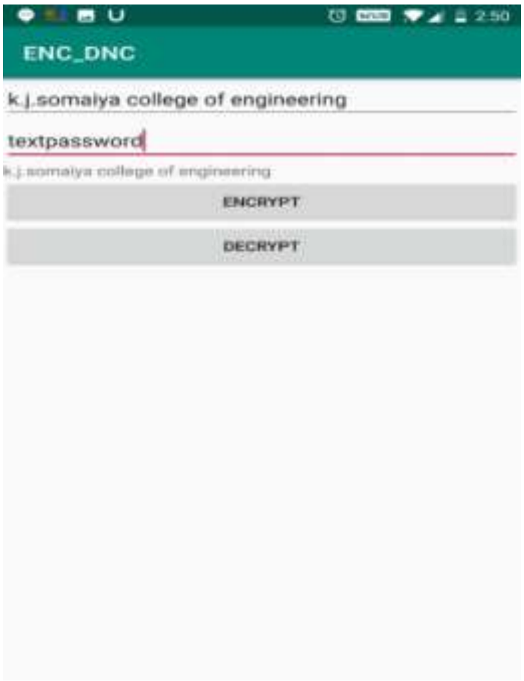


k.j.somaiya college of engineering

textpassword

VadbeVnntgerzbIYR+yqDmt8W80/3zrvOK2W4IWSpUncusLn4IET WLmN2ZLMr5IW

Fig: 2.Encrypted Message


ENC_DNC

k.j.somaiya college of engineering

textpassword

k.j.somaiya college of engineering

Fig: 3.*Decrypted Message*

Bluetooth (IEEE 802.15.1)

Bluetooth is a short range wireless communication technology that allows transmission data or voice from one device to another device. IEEE 802.15.1 is IEEE standard of Bluetooth. The purpose of a Bluetooth is to replace the cables and connect the devices wirelessly. Bluetooth devices can form small networks called ‘piconets’. It is a network of devices connected using Bluetooth technology two or more units sharing the same channel. ‘Piconets’ is a very small network so it's called ‘Piconets’.Bluetooth Security Issues are Authorization, Authenticationand Authentication. Pairing is one type of Authentication.The purpose of pairing is to determine whether the capability is are on each end of the two devices getting ready to pair.There are four different pairing methodNumeric Pairing, Just Work, Passkey Entry, Out Of Band using this method we can secure the Bluetooth Environments.

HYBRID LEVEL SECURITY ISSUES

This category is a combination of the software and hardware based mechanisms to maximize the security efficiency. It is the best way to ensure efficiency and flexibility but it requires more efforts for communication between hardware and software teams to ensure the compatibility between the two products.

Example, the developer used not only software and hardware approach to map a public key cryptosystem but also compiler based software tool on-chip hardware components. The hardware components are used for security and software components are used hide security information to escape reverse engineering.

Framework for IoT Security

Framework for IoT security covers six levels. The six phases are: device startup security, access control, authentication and authorization, detect and control and the last step is updates and recover.

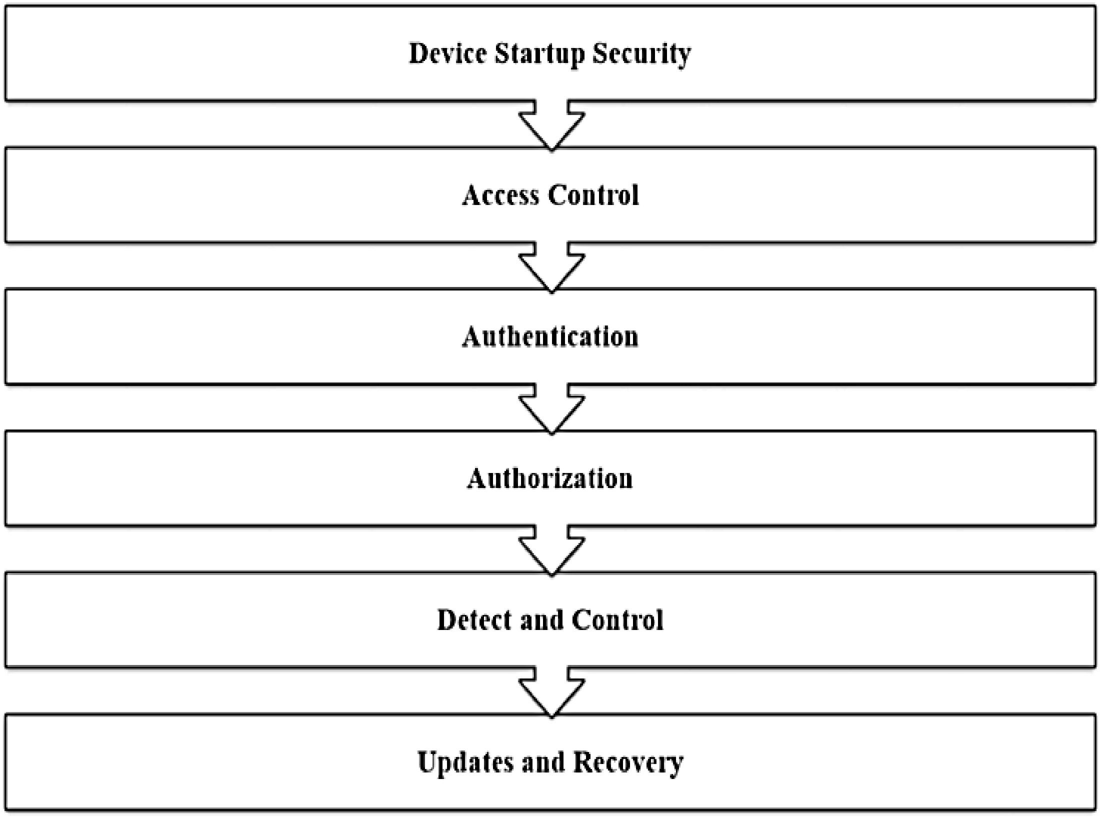


Fig: 4. *Framework for IoT Security*

Device startup security

This phase is required to make sure all the software programs and operating system are verified and allow to run system device. Example, digital signature.

Access control

Access control mechanism should be execute in order and make sure that all devices component and software applications have limited access.

Authentication

All devices are connected to network. The system should identified and give some proofs to network. Network checks all proofs valid or not, if all proofs are correct then systems connect to right network. Username and password are used for securing devices and software applications. Handling this phase carefully is necessary.

Authorization

This phase check ensures devices should be connected to correct network. The information being exchanged between device and network, a trusted relationship should establish.

Detection and control

The device starts a receiving data from networks. Controller mechanism is used to monitor a traffic and alerts. After receiving all alerts, detection control mechanisms take a decision which threats are harmful for system.

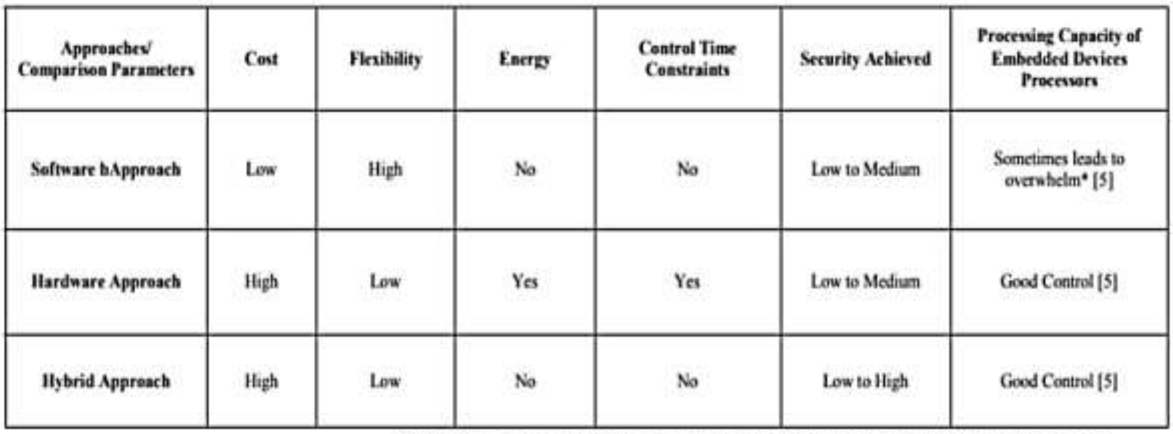
Update and recovery

Update and recovery are also necessary to make sure all functionality of devices should be up to the mark.

COMPARATIVE STUDY

Comparison of Short-Range Wireless Technology

***Table: 1.** Comparison between Different Approaches.*

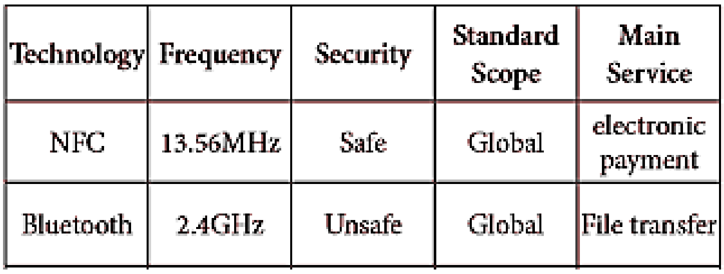


Approaches/ Comparison Parameters	Cost	Flexibility	Energy	Control Time Constraints	Security Achieved	Processing Capacity of Embedded Devices Processors
Software hApproach	Low	High	No	No	Low to Medium	Sometimes leads to overwhelm* [5]
Hardware Approach	High	Low	Yes	Yes	Low to Medium	Good Control [5]
Hybrid Approach	High	Low	No	No	Low to High	Good Control [5]

*Some methods that use software approach run many tasks at the same time, this leads to deadlock that may lead to overwhelm the processor.

Table 2 shows NFC and Bluetooth both are software based short-range wireless technology. NFC works on 13.56MHz and Bluetooth works on 2.4GHz frequency. NFC is more secure than Bluetooth, both standard scope are global. NFC main service is electronic payment and Bluetooth main service is file transfer.

***Table: 2.** Comparison of Short-Range Wireless Technology.*



Technology	Frequency	Security	Standard Scope	Main Service
NFC	13.56MHz	Safe	Global	electronic payment
Bluetooth	2.4GHz	Unsafe	Global	File transfer

Table 2 shows a comparison between three security level approaches of flexibility, cost, time control constraints, energy and processing capacity of embedded device processor. Software approach is a cost effective and flexible as compared to hardware and hybrid. The hardware approach requires more energy and control time constraint as compared to software and hardware. In Hybrid approach security is high and processing capacity is also good. The hybrid approach is the best as compare to other approaches because it's efficient, flexible and more secure.

CONCLUSION

The fundamental security models are confidentiality, availability and integrity. To get a complete secured device, fundamental security models should be analysed. IoT is a successful beneficial technology for manufacturers and customers. There is lots of security flaws occur in IoT enable system. However security flaws are categorised in three levels (Hardware level security, Software level security, Hybrid level security). Hardware level security, we need to secure the 'things' in devices. Software level security, we need to secure the network and things in the systems. Hybrid level security, using IoT security framework we can secure the IoT environment. The hybrid is a combination of software and hardware. It can be conclude that best approach for securing IoT environment is a hybrid one because hybrid is a more secure, efficient and flexible as compared to software and hardware.

REFERENCES

1. Jean Pierre Nzabahimana, “Analysis of Security and Privacy Challenges in Internet of Things,” The 9th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT’2018 24-27 May, 2018, Kyiv, Ukraine.
2. SubhaKoley, PrasunGhosal, “Addressing Hardware Security Challenges in Internet of Things: Recent Trends and Possible Solutions” IEEE DOI 10.1109/UICATC-ScalCom-CBDCom-IoP.2015.105.
3. AmiraHagag Imam, “Internet of Things Security Framework,” IEEE 978-1-53864266-5/17/ 2017.
4. Mrs.SnehalDeshmukh,“Security Protocols for Internet of Things: A Survey,” IEEE 978-1-5090-5913-3/17/

Cite this article as: Pooja V. Chavan. (2018). Analysis of Hardware and Software Security Challenges in IoT. Journal of Web Development and Web Designing, 3(3), 21–27. http://doi.org/10.5281/zenodo.2267384