International Engineering Journal For Research & Development
Vol.4
Issue 5

E-ISSN NO:-2349-0721

Impact factor : 6.03

THE RISKS AND LIMITATIONS OF SECURITY MECHANISMS ON IOT ENVIRONMENTS

Ms. Shilpa B. Sarvaiya
Department of Computer Science
Vidyabharati Mahavidyalaya, Amravati
sarvaiya.shilpa@gmail.com

Dr.Swati S.Sherekar
PG Dept. Of Computer Sci & Engg.
S.G.B. Amravati university,
SS_Sherekar@rediffmail.com

Dr.V.M.Thakare
HOD, PG Dept. Of Computer Sci. & Engg.
S.G.B. Amravati University, Amravati
vilthakare@yahoo.co.in

ABSTRACT

Internet of Things is the technique which is provided by the unique identifiers that can automatically transfer the data over the wide network without the help of human being. The devices uses are vulnerable to hack. The purpose of hacking the devices of Internet of Things may not be accessing data only, but it could be harming the users of those devices. In other words, it might affect them economically, endanger their health or put their lives at risk since this technology is directly connected to their daily lives, and this is considered a violation of users'privacy.The devices of Internet of Things are hacked and exploited in order to attack the Internet infrastructure supplied by some major companies. In this paper we have token an overview about the security of Internet of Things, we are trying to cover the possible security measures to put a stop to attacks from the previous research scholars on the topic of security of Internet of Things. We propose a one of a kind concept of three Layered Security to prevent the malicious activities of Cyber-criminals. In these three layers we have ponder the Device Security, Communication Security and Server Security. Risks and Limitations are also discussed here.

Keywords-IoT Security; Three layered Security; Network Security; Risks; Limitations

1. Introduction

Internet of Things (IoT) is considered as an integrated part of Internet, also defined as a global network infrastructure and dynamic composed of a large number of objects, able to communicate and interact with each other, with end users [1, 2, 3].These objects must have unique identities which allow interactivity. Firewalls cannot be being embraced within embedded systems. The appealing targets of hackers and cyber-criminals are embedded computing devices. The very last lessons and hacking occurrences in Internet of Things have challenged the security expert professionals. The PC security ways out could not provide complete solution for the security to be as long as for Internet of Things. The significant functionality of Internet of Things has given much wider scope for the cyber-attacks and leaded to catastrophic punishments. Duplication is widely found in embedded devices for the hacker. If the cyber-criminal could find the methodology or cracking mechanism for one, it can be applied to all replicated devices and leads to great havoc. Many people believe that the cryptographic algorithms enforcements alone provide the security. Some investigators could implement the cryptographic protocols as a 2nd kind of link in Internet of Things. Much the same implementing of technology knows how to minimize the risk of the physical attacks in IoT will be adequate enough to security in Internet of Things. Implementing UVEEPROM or Flash erasure or Laser glitching or Laser Assisted power analysis can be certain of the security for IoT.As the matter of fact, the implementation of any security measures cannot give most appropriate security to the IoT so much further. The cyber criminals have somehow broken the security layers and instigating the attacks [4].This paper is organized as follows. In section 2, we presents the related work, section 3 a proposed security model according to areas of interest to today worked in IoT is presented, section 4 describe risks in IoT respectively, section 5 discuss result and analysis. The final section 6 conclusions and future work is presented. To suggest highly a novel security distinguishing with three layered security for Internet of Things.

2. Related Work

The rapid development of information technology and Internet security information about IoT, a new problems and potential security over information has been rise. Therefore, it becomes a focus aspect to build a safety and reliability system in the IoT context.IoT has knowledgeable the logical attack surface. These attacks have been successfully picked up by the TCB of devices involved architecture with wider perspective has given enough security measures for the attacks.IoT is wealthy with complex software and rich operating systems. The amplified security is essentially gad to have to provide the protection against the surface attacks. This has been effectively encountered by the Logical TCB conducting [4].

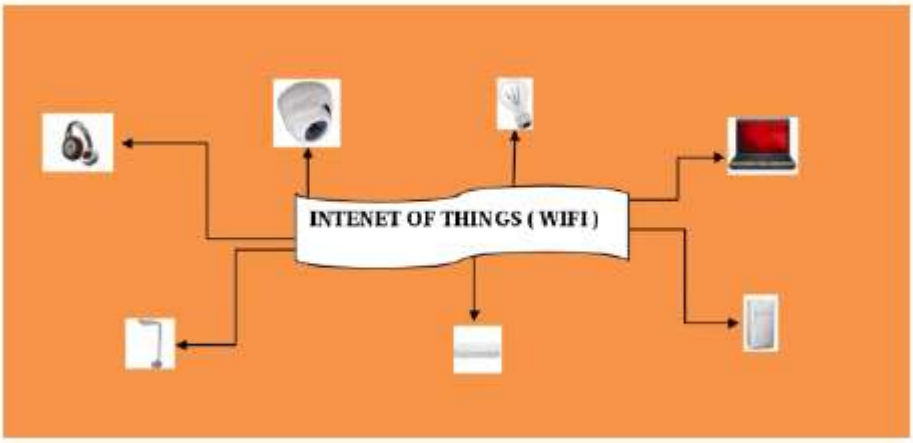

Figure 1: IoT Security Provision.

The Internet of Things is a virtuousness hacking target for all widespread cyber-criminals. The motor vehicles and transportation systems which are working with the Internet of Things are the pinnacle targets for hackers. They have already call attention to their attacks and did prospective damage to the automobile segment. Symantec firm has advised a protecting code embedded in the drives of IoT.This code makes it possible for the devices to work against the hacking technology and will not uncover the way for incursion [2].

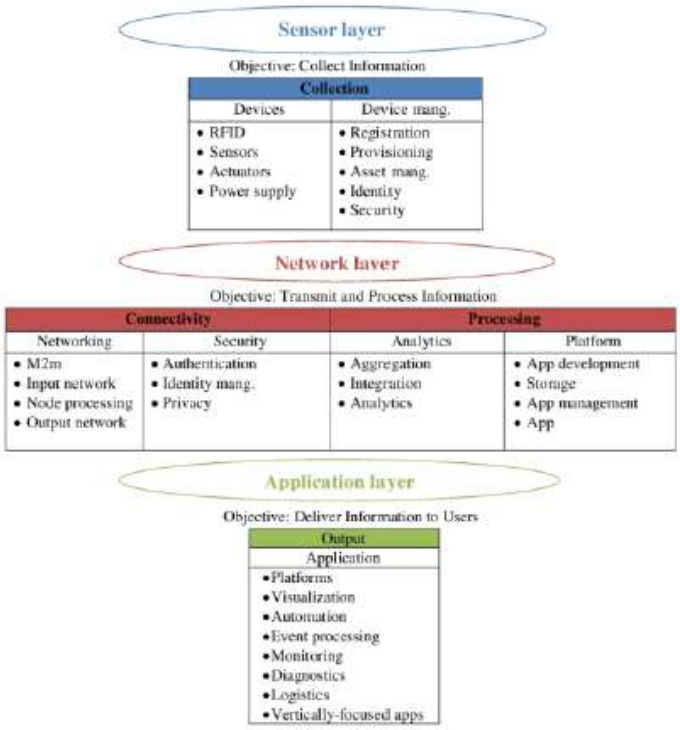

Figure 2: Three layered Security

The three layered security implementations of IoT operations of any kind of system. The security implementation is developed and framed in a three-layer framework for the IoT security to implement the safe and secure operation of remotely performing controlling and monitoring operations of the users for the targeted devices. The proposed security model is describe below.

3. Security Model Proposed

Due to Internet of Things is a large field with various technologies, a categorization of the issues and technologies was made, this categorization is the basis for analysing some detail of security and privacy in the respective fields. Figure 3 shows a categorization of the issues and their respective technologies used in each of the topics that make up the Internet of Things. According with figure 3, it can be identified eight major areas within IoT which must be specified level of security related studies .They are describe below [5].

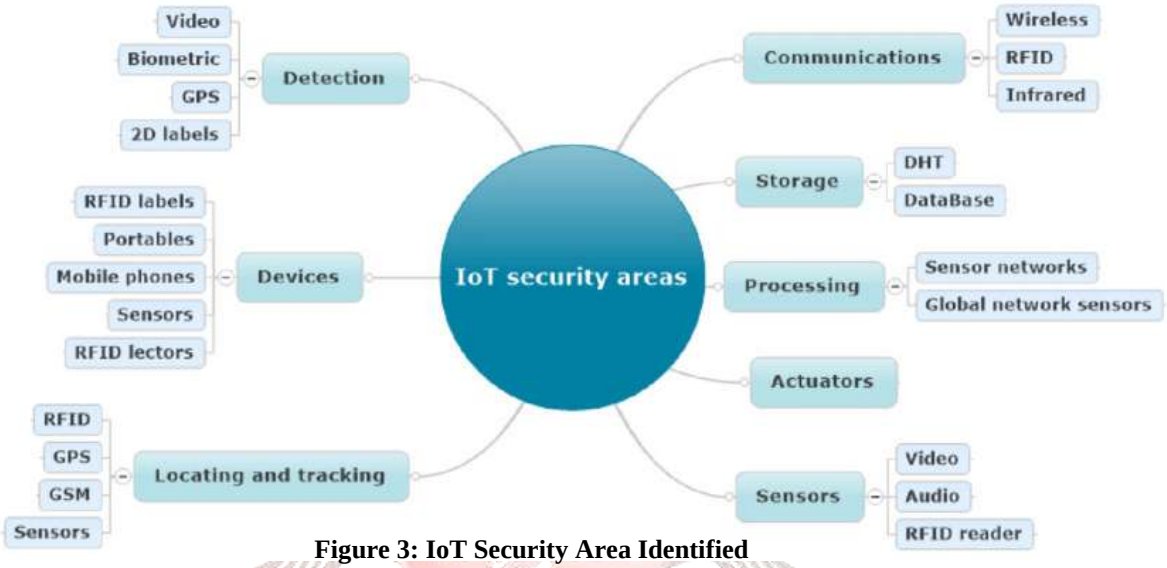

Figure 3: IoT Security Area Identified

1. Communication: Research on communication protocols has come up with solutions that provide the integrity, authenticity and confidentiality, such as TLS or IPsec. Privacy needs have been addressed by different routing schemes as Onion Routing or Free-net, but these are not widely used.

2. Sensors: Integrity and authenticity of the sensor data is an objective of the current research. The confidentiality of data sensors is a very vulnerable condition therefore the need for confidentiality in the sensor is low, so that confidentiality is based on the confidentiality of communication. Mechanisms such as face blurring video data are important to implement in order to preserve the privacy of individuals and objects. Sensors availability depends mainly on the communication infrastructure. Regulations are necessary to preserve the privacy of individuals who are currently most often unconscious on the sensors, such as video cameras.

3. Actuator: Integrity, authenticity and confidentiality of data in an actuator depends primarily on the security of communications.

4. Storage: Security mechanisms for storage devices are well established. Data storage is highly sensitive to privacy and there are many cases of violation of privacy regulations should be widely distributed to provide an adequate response to user privacy protection. Storage availability depends mainly on the availability of the communication infrastructure and well-established mechanisms for redundancy storage.

5. Devices: Within the field of integrity of the devices, a device is free from malware. This property has also been called ‘’admissibility’’ a presently open issue, researched Trusted Computing Platform (TPM) and highly sensitive. The authenticity of a device handles all the communication parts, not seen such as the end point of connection .Confidentiality is a device with integrity to ensure that no third party has access to internal data devices. Devices privacy depends on the physical privacy and privacy of communication.

6. Processing: Integrity in data processing services is based on the integrity of communication devices. Also, it depends on the design and proper execution of algorithms for processing. The authenticity of processing depends solely on the authenticity of the device and the authenticity of the communication. The property of confidentiality in processing depends only on the integrity of the device, and in the case of distributed

processing, depends on the integrity of the communication. The availability of processing depends on the device and the availability of communication exclusively.

7. Location and Tracking: The integrity of Location and Tracking is based on the integrity of Communication and the integrity of the reference signals used in the location, such as GSM or GPS.It also depends on the authenticity of the authenticity and integrity of communication devices. The confidentiality of data tracking and tracing are of great importance to ensure user privacy and therefore is very sensitive. Confidentiality in this context means that an attacker is not able to disclose the location data and therefore is primarily based on the confidentiality of communication. Data privacy location means that there is no way for an attacker to reveal the identity of the person or object and the location and tracking is not possible without the agreement or explicit knowledge.

8. Identification: It uses same sensitivities than Location and Tracking. One difference is the higher sensitivity on the integrity part. It is easier for an attacker to manipulate the identication process as it is handling the localization process. This translates mainly due to technology used (eg RFID or Biometrics) is more likely that an attacker manipulate location technologies (eg GSM).From this basic classification criteria are defined to determine the relevance of the security level on each of the areas identified in table 1.

Table1: Recommendation Criteria in Security Areas

Properties	Security Principles					
	Integrity	Authenticity	Confidentiality	Privacy	Availability	Regulation
Communication	High	High	High	Medium	High	Low
Sensors	High	Medium	Low	High	Low	High
Actuators	Low	Low	Low	Medium	Low	Medium
Storage	High	Medium	High	High	Low	High
Devices	High	Low	Low	Medium	Medium	Medium
Processing	Medium	Low	Low	High	Low	High
Location and Tracking	Low	Low	High	High	High	High
Identification	Medium	High	High	High	High	High

Recommendations

1. It is highly recommended to incorporate the security at the design phase of IoT of a specific device.
2. It is highly recommended to promote security updates and vulnerability management for the proposed IoT.
3. It is highly recommended to apply the TLS and DTLS data encryption for the data transmitted in IoT management.
4. Authentication and key management is a mandatory solution to be followed by IoT users.
5. The strong communication should be established with the system and the devices that are operated in IoT regardless of manufacturer of the devices.

4. Risks in Internet of Things

Any device connected to the Internet like a smart car, a camera surveillance and a smart lamp, which has its own system that performs a specific task. It is apt to hacking more than computers because their security system is extremely weak. The most significant problems are summarized as follows [6]:

1. Privacy problems that might put the user data at risk, however this data is considered too sensitive.
2. Material damage that could be caused by tampering with instruments which can lead to harming the user, such as home appliances.
3. Misusing this technology for purposes like monitoring users and violating their privacy.
4. Possibility of exploiting location data of those devices for example determining the car site.
5. Exploiting those internet devices for hacking electronic governments and major companies that are associated with the Internet.

4.1 Security vulnerabilities of Internet of Things

1. Vulnerabilities in communication interfaces between the user and Internet of Things is insecure, where the user can bypass, access and control the device.
2. Weakness in the authentication process [7].
3. There are not enough methods to identify the authorized users, and this allows unauthorized people to log in to those devices.
4. Insecure software occurs when programmers focus only on the speed of transfer data neglecting the security aspect.
5. Using insecure protocols for data transfer.
6. Easiness of scanning and knowing the devices connected to the Internet.

4.2 Possible solutions to reduce risk

1. Default passwords and ideally default usernames to be changed during initial setup.
2. Ensuring user accounts cannot be enumerated using functionality such as password reset mechanisms.
3. Ensuring account lockout after 3-5 failed login attempts.
4. Ensuring the cloud-based web interface is not susceptible to XSS, SQLi or CSRF.
5. Ensuring credentials are not exposed over the Internet.
6. Implement two factor authentications if possible.
7. Implemented Secure Sockets Layer (SSL) and Transport Layer Security (TLS).
8. Automatic update IoT devices with security patches when packages update become available.
9. Disable Universal Plug and Play (UPNP) protocol for prohibit from discover hacker to know devices in your network.
9. Most devices exploit by mira virus must be updated firmware.

5. Result and Discussion

Implementation of security architecture for every devices connectivity with the internet servers to protect the systems from possible attacks from Cyber-Criminals or hackers. The security architecture should consist of device manufacturing specifications as well as the system specification to have proper integration and transparency over the devices and servers [8, 9].

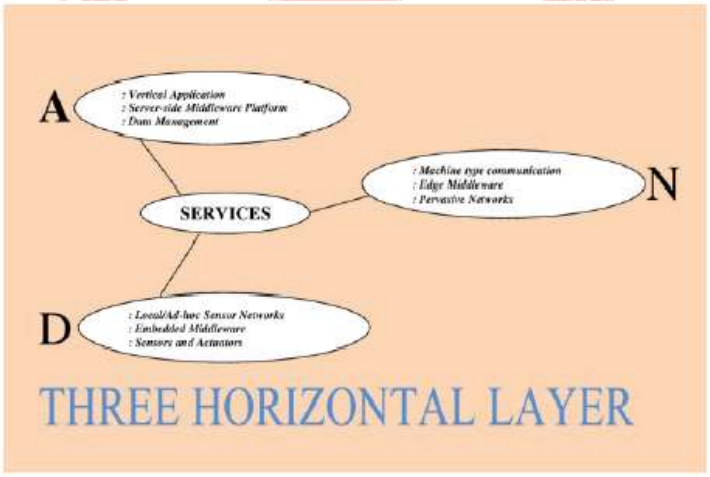

Figure 4: Three layered Security.

The three-layer security should be implemented at Device Level, Communication Level and finally the Server Level. The security updates against the possible attacks and unknown vulnerability should be continuously done. The management should always implement build on proven security practices needed for IoT implementation for specific device management. The transparency should be maintained between the operation of IoT developers, IoT devices manufacturers, communication providers and industrial and business-level consumers [10, 11].

Taking advantage of the security for IoT is the aspiration of the project. The proposed fitting solution is meted

out in three levels. The security implementation is at Server Level is the first juncture. The 2nd level is implementing the vastly level security in Communication layer. Finally, the 3rd level security is ought to be implemented at Device Level. The security level at virtual servers will be conjunct with the Cloud Computing servers. Each of these servers are operated by the remote users to control over the devices and gadgets. Above and beyond the cloud server's security the increased security needs to be implemented in the Server Level with formidable authentication and authorization with digital encryption standards. The second level security must have to be implemented at Communication Level. The communication effectively between the servers and users and the communication between the servers and devices are predominant. The security implementation need to be incorporated at Communication layers of the IoT operations. This implementation can be done with incorporating network security algorithms and strong admeasures for external attacks. The proposed solution is stressing on the third level security at Device Level. The devices embedded with chips to store the software should also implement with the anti-virus and protection against the vulnerabilities and external attacks to compromise the devices. The devices are same and connected in multiple number with the servers. If the attacker compromise one single device can easily compromise other devices. Hence the Device Level security is equally important in IoT operations.

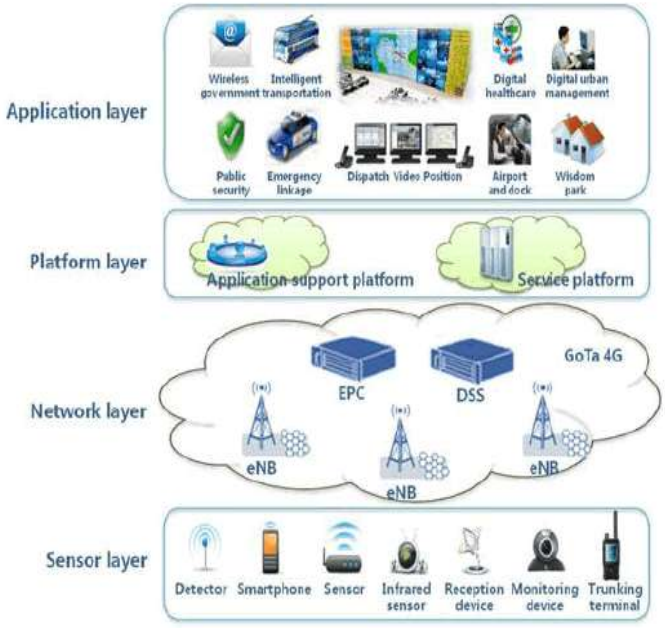

Figure 5: Security Integration Points in IoT.

6. Conclusion

The goal of this paper shows what has happened and maybe happen in the future as well as the work of the crisis precautions to reduce risk. The aim of the paper is to suggest the three-layer security implementation for the IoT working mechanism. In this paper the possible high-level security implementation has been suggested at Device Level, Communication Level and Server Level. In addition to that the mandatory implementation of security monitoring and updating the security implementations time to time to prevent the attacks in IoT.Finally, the paper has recommended the possible precautions to implement strong security in IoT.As future work, is foreseen to carry out a characterization of these problems, so that from an ontological model and intelligent agents it can be carried out the appropriate identification of security mechanisms from most frequent problems in the IoT environments. This would facilitate security alternatives identification, deployment access models IoT devices first.

7. References

[1] Ms .B.Sarvaiya, Dr.S.S. Sherekar, Dr.V.M.Thakare," Study of Security Challenges in Multi-layered Structure and Various Attacks on IOT", AIC 2K18 Annual IETE Convention International Journal of Electronics, Communication And Soft Computing Science & Engineering (IJECSCSE),Impact Factor- 4.526, ISSN 2277-9477, 29 and 30 September-2018.

[2] Ms.S.B.Sarvaiya, Dr.S.S.Sherekar,Dr.V.M .Thakare," Taxonomy of Authentication Techniques in Security Attacks of Internet of Things", NCETS "Research Journey" International E- Research journal, Impact Factor-6.261, ISSN: 2348-7143,February-2019

[3] Ms.S.B.Sarvaiya, Dr.S.S.Sherekar, Dr.V.M .Thakare," Internet of Things Security Architecture: Challenges and Issues", Recent Advances in Science and Technology (RAISAT-2019), Impact Factor -5.5, ISSN: 2277-5730, 5 and 6 March-2019.

[4] Tamanna Siddiqui,Saif Saffah Badr Alazzawi," Security of Internet of Things", International Journal of Applied Science-Research and Review,Vol.5,No.2.8,ISSN:2394-9988,iMedPub Journals May 31,2018.

[5] Paulo Gaona Garcia, Carlos Montenegro Marin, Juan David Prieto, Yuri Vanessa Nieto,"Analysis of Security Mechanisms Based on Clusters IoT Environments. "International Journal of Interactive Multimedia and Artificial Intelligence, Vol.4, No.3, IEEE 2017.

[6] Mohammed Tawfik, Ali M.Almadni, Alhasan A.Alharbi, "A Review: The Risks and Weakness Security on the IoT." ,International Conference On Recent Advances In Computer Science, Engineering And Technology,IOSR Journal of Computer Engineering (IOSR-JCE),e-ISSN:2278-0661,p-ISSN:2278-8727,pp 12-17, IEEE 2017.

[7] M.U.Farooq, Muhammad Waseem, Sadia Mazhar," A Review on Internet of Things", International Journal of Computer Applications, ISSN: 0975-8887, Vol.113, No.1, IEEE, March 2015.

[8] B,Yan, T.S.Lee, T.P.Lee," Mapping the Intellectual Structure of the Internet of Things, a co-word analysis,"Scientometrics,Vol.105,No.2,PP.1285-1300,Sept 2015.

[9]Shagufta Rajgurul,Swati Kinhekar,Sandhya Patil, "Analysis of Internet of Things in a Smart Environment.", International Journal of Enhanced Research in Management and Computer Applications,Vol.4,Issue 4,ISSN:2319-7471,April 2015,PP 40-43.

[10] J.Granjal,et al.," Security for the Internet of Things: A Survey of existing protocols and Open Research Issues",Communications Surveys & Tutorials,IEEE,Vol.17,PP. 1294-1312,IEEE 2015.

[11] D.Pavithra,R.Balakrihnan," IoT Based Monitoring and Control System for Home Automation",Global Conference on Communication Technologies(GCCT),PP.169-173,IEEE 2015.