Research Article

iMedPub Journals
www.imedpub.com

International Journal of Applied Science - Research and Review
ISSN 2394-9988

2018
Vol.5 No.2:8

DOI: 10.21767/2394-9988.100073

Security of Internet of Things

Tamanna Siddiqui* and Saif Saffah Badr Alazzawi

Department of Computer Science, Aligarh Muslim University, Aligarh, India

***Corresponding author:** Dr. Tamanna Siddiqui, Department of Computer Science, Aligarh Muslim University, Aligarh, India, E-mail: ja_zu_siddiqui@hotmail.com

Received date: April 19, 2018; **Accepted date:** May 25, 2018; **Published date:** May 31, 2018

Citation: Siddiqui T, Alazzawi SSB (2018) Security of Internet of Things. Int J Appl Sci Res Rev Vol.5 No.2:8.

Copyright: © 2018 Siddiqui T. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Abstract

Internet of Things is the new age paradigm concerned with devices and networks through Internet. The widespread of devices and other objects to be managed can be called as things. In this field an advancement is to truly perform the software assisted operations from out of the way areas controlling. This advanced operations needs lots of layers of deterrence. It necessitates to map out the strongest layer of incorporation embedded with firewalls, authentication/encryption, security protocols and instructions detection and intrusion prevention systems.

In this paper we are trying to cover the possible security measures to put a stop to attacks from cyber-criminals with add measures. The most likely add measures are well given approval by 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.

Keywords: Internet of Things; Security; Cyber-attacks; Three layered Security

Introduction

Firewalls can't 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 so 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 can't give most appropriate security to the IoT so much further. The cyber criminals have somehow broken the security layers and instigating the attacks [1].

Industrial and manufacturing and marketing realms are using the IoT devices to monitor and control the equipment used on a regular basis operation. Furthermore, Healthcare associations is inevitably relying on the IoT connected medical devices to manage remotely from another country by the most experienced and versatile doctors (**Figure 1)**.

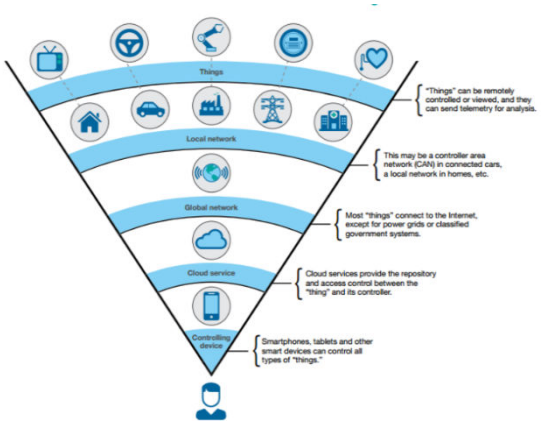

Figure 1 IoT Security architecture.

Car and truck industry is giving significance value to the customers by supplying the IoT services to the vehicles purchased. IoT devices used in all industrial sectors are wireless and treated remotely. At this juncture the crooks or hackers will break the track of connectivity with the end user

of IoT and took control over the devices. This state of affairs can leads to unaccountable loss to the owner of the devices that are interrelated. To refrain from these conditions for sure security principles have been indicated with the implementation of basic security principles of Confidentiality, Integrity and Availability [2]. The major goal of the paper is to provide an appropriate solution with elevated security to the devices participating in the operations Internet of things by integrating the data security, authentication, secure communication protection against cyber-attacks. The idea of desired outcome of the paper is to investigate the achievable security measures for the devices and components involved in Internet of Things. Getting acquainted with previous research papers and international journals about the cyber-attacks and admeasures for Internet of Things. Exploring the contemporary solutions suggested for the latest attacks on IoT.

To suggest highly a novel security distinguishing with three layered security for Internet of Things.

Related work

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 had to have to provide the protection against the surface attacks. This has been effectively encountered by the Logical TCB conducting [3] (**Figure 2)**.

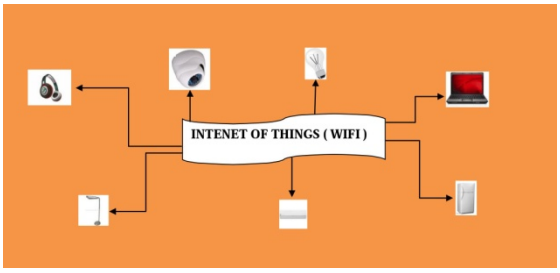

Figure 2 IoT Security provision.

GSM society has presented solutions for some critical either against IoT security implementation. They offered answer to the problem for wrestle cloning in IoT with the authenticating an end point identity. The endpoint identity can be responded with carry out the trusted Computing Base, implementing trust Anchor, carrying out of Tamper Resistant Trust Anchor and implementing an API for using the TCB associated with the scientifically proven Random Number Generator. The defy against the Trust Anchor can be efficaciously encountered with the consideration of Supply Chain Security, Personalize endpoint Device prior to accomplishment, exclusively provision for each endpoint. In anticipation to the question of reduce the potentiality of Impersonation might be effectively encountered with the implementation of Endpoint Communication Security, Fabulous Forward Secrecy and by using proven random number generator with the authorization of metadata harvesting [4].

Tata Consultancy has awarded tamperproof IoT design and implementation in its acknowledge. While they are implementing the preferred IoT with device enactment and deployment should be implemented. The fitting solution design can be given in unison with the user terms and conditions of estimating the possible hazards and attacks forecast. The IoT of things must be distinctively guarded with the possible continuous support against the threats and attacks [5] (**Figure 3)**.

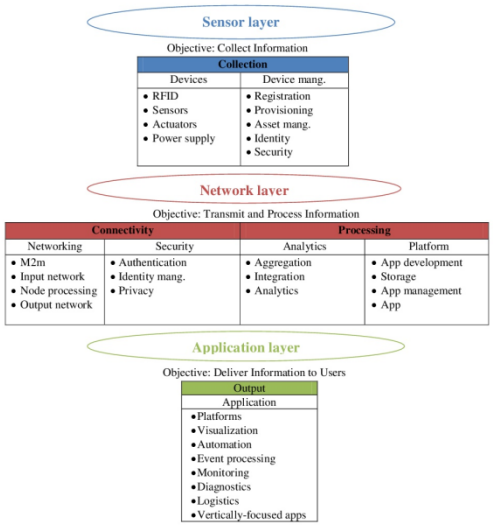

Figure 3 Three layered security.

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].

Proposed security architecture and solution

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 3d level security is ought to be implemented at device level. The security level at virtual servers will be conjunct with the cloud computing servers. The IoT implementation basically done with 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 easily. Hence the device level security is equally important in IoT operations.

The proposed system is enriched with three layered security implementations of IoT operations of any kind of system. The proposed 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 system methodology is described below.

Methodology

IoT implementation would be a great task with the tight security implementations. IoT is the hot target for all hackers, Cyber-criminals. A significant vulnerability always trying to break the communications between the end use and the end point of the device connected in IoT. The cyber-criminals are not concentrating the physical accessibility of the devices. They are always trying to break the communication networks and take control of the devices remotely and implement the hacking mechanism [6].

In this paper we suggest three security principles in three-layer security to prevent the possible security threats and attacks from cyber criminals. Implementation of robust and tamper resistant storage of cryptographic keys integrated with the cryptographic functions should be in the first layer. The standard and secured communication should be established between the device and the IoT operator. The hardware used in the IoT process should be embedded with the security focused mechanism. The communication network should be enriched with the protection rules and shielding techniques against both virtual and physical attacks [7].

Results and Discussion

Implementation of a 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 [5] (**Figure 4)**.

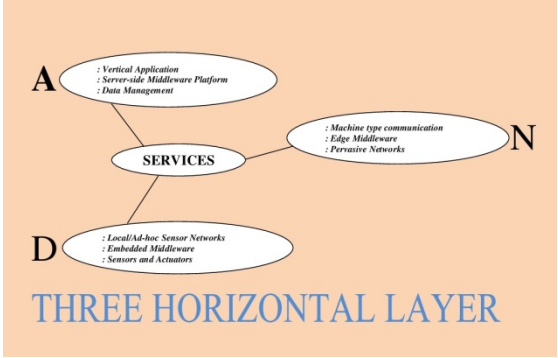

Figure 4 Three layers of IoT.

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 operations of IoT developers, IoT device manufacturers, communication providers and industrial and business-level consumers [8-11] (**Figure 5)**.

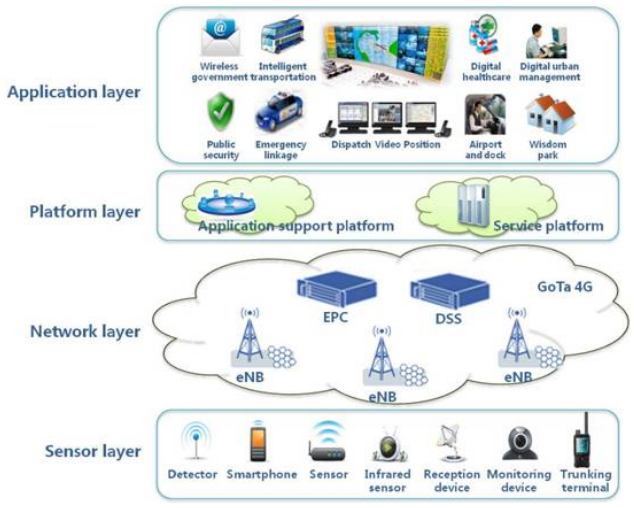

Figure 5 Security integration points in IoT.

Recommendations

- It is highly recommended to incorporate the security at the Design phase of IoT of a specific device.
- It is highly recommended to promote security updates and vulnerability management for the proposed IoT.

© Copyright iMedPub

- It is highly recommended to apply the TLS and DTLS data encryption for the data transmitted in IoT management.
- Authentication and Key management is a mandatory solution to be followed by IoT users.
- The strong communication should be established with the system and the devices that are operated in IoT regardless of manufacturer of the devices.

Conclusion

IoT is the hot target for the Cyber-criminals. This paper has illustrated the possibility of attacks in various levels of Inter of Things operated remotely by the users to control and monitor the devices. 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 system 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.

Competing and Conflicting Interests

The author declares no conflict of interest related to this work.

References

1. Dave R (2016) Tackling data security and privacy challenges for the internet of things. w3c Web of Things IG Meeting in Beijing.
2. Lin H, Bergmann NW (2016) IoT privacy and security challenges for smart home environments. Information 7: 44.
3. Dominique B (2016) Proven security for the internet of things. Embedded World Conference.
4. IoT Security Guidelines Endpoint Ecosystem. Version 1.0, 08 February 2016, Copyright © 2016 GSM Association.
5. Tata Communications (2017) HPE to work with Tata Communications to build world's largest iot network in India to enhance resource utilization.
6. Internet Society (2015) The internet of things: An overview.
7. https://iotsecurityfoundation
8. Dell (2017) Security for the internet of things.
9. Symantec (2016) An internet of things reference architecture.
10. US Department of Homeland Security (2016) Strategic principles for securing the internet of things (IoT).
11. Embedded Hardware Security for IoT Applications (2016) A smart card alliance internet of things security council white paper.