Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 6.017

IJCSMC, Vol. 8, Issue. 4, April 2019, pg.01 – 06

A Review on Secure Channel Establishment Technique to Increase Security of IoT

Pankaj Gulati; Amandeep Verma; Dr. G.N. Verma
I.K. Gujral Punjab Technical University

ABSTRACT: The internet of things is the decentralized type of network in which no central controller is present due to such type of network routing is the major issue. In the previous research various authors has proposed techniques which increase security of IoT. In this review paper, various techniques correspond to security issues are analyzed in terms of certain parameters.

Keywords: Internet of things (IoT), security, Encryption, Privacy, authentication, key management, Security Challenges, Secure Channel.

I. INTRODUCTION

The Internet of Things (IOT) is an organic network of related physical things that are open through the web and joined with contraptions, programming, sensors which engages to interface and exchange data, making open entryways for organize blend of the world into PC based structures, realizing profitability change, money related favorable circumstances and diminished human undertakings. It incorporates extending web accessibility past standard contraptions, to any extent of generally nitwit and normal articles. Advancement introduced contraptions can without a lot of a stretch pass on and coordinate over framework and they can be remotely checked and controlled as well. Distinctive exercises are supported by IoT applications remembering the true objective to give successful correspondences like change in capability, more lifted measure of execution and ensured security gave inside IoT advancement applications [1].

II. CHALLENGES

Even though there are variety of advantages found in IoT, these systems also face many issues within them. Some of the commonly found issues are:

a) *Security:* Various devices that communicate amongst each other across the networks can be provided by an ecosystem present in IoT. Without providing any security related constraints, there is very less control provided by system. There are different kinds of attackers present in the applications which can attack the users.

b) Privacy: There is a complete detail of information present in personal data of IoT users which needs to be protected from the attackers [2]. This can be done with the assistance of precise measures.

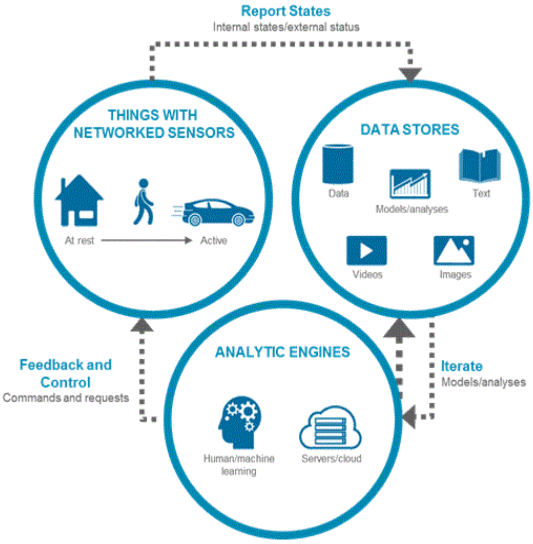

Figure 1: Interaction between devices of IoT.

c) *Complexity*: In terms of design, maintenance and implementation, the IoT systems can be complex within certain applications. These applications might include some complex level of technologies within them which can sometimes be an issue.

d) *Flexibility:* The flexibility of IoT systems is a major concern in some of the applications. This issue mainly arises when the systems are to be integrated with each other. Within various conflicting systems the IoTs can be involved due to which many issues might arise.

e) *Compliance*: There is a need to provide particular regulations within the IoT technologies as well. In case when there are many standard software compliance present that are competing against each other, the complexity might increase to greater extent.

III. SECURITY

There is a possibility of allowing larger number of attackers to enter within the IoT systems when any device connects with them. Even within single small sized device there are broader vulnerabilities present. There are huge amount of risks present within the IoT systems which are mainly caused during the transferring of data, accessing of devices, or making connections amongst the devices. Thus, the major security issues arise while producing devices with minimal cost and higher number of devices. Due to this, there is an increase in chance of attacks in the systems. Some other related security issues that arise within IoT are [3]:

a) Unpredictable Behavior: The behavior of technologies that are emerging cannot be predicted previously. This is mainly due to the fact that there is large number of devices being deployed regularly and consistently. There can be a proper designing of the system which can be in proper control of the administration. However, the guarantee that this system might interact with other systems cannot be provided here.

b) Device Similarity: There is uniformity amongst the IoT devices. There is similar technology and components utilized by these systems. There are many other issues faced by the systems when there is one system only which is facing any kinds of vulnerability issues.

c) Problematic Deployment: The placement of advanced networks and analytics within the IoT systems is the major goal of these systems. The issue related to securing the devices are physical manner is however, caused within such scenarios.

d) Long Device Life and Expired Support: The longevity of IoT devices is an important advantage in these systems. However, this characteristic also means that they might outlive the supporting device as well. The traditional systems that have support and require updations after frequent times are compared with the new enhanced systems [4]. There is an absence of similar level of security within the excluded systems in comparison to newly enhanced systems.

e) No Upgrade Support: No upgrading or modification is required within various IoT devices present within IoT. However, if some devices require any upgrades, the owners ignore them.

f) Poor or No Transparency: Transparency related to the functionality of the IoT devices is not able to be provided in proper manner. The processes going on cannot be observed or accessed by the users. Thus, the users only can assume on how the devices work. The unwanted functions or the gathering of data cannot be controlled by the users. Many functions that are not required by the user might be added in the system during the updating processing of device by the manufacturer.

g) No Alerts: The facility of providing incredible functionality within the IoT is a major objective to be achieved [5]. The awareness of user is required here which again generates the similar kind of issue. It is not known to the users whether what processed is going on in the devices. Thus, there are various security issues that remain undetected within these systems.

Different approaches are being employed for secure End-to-End communication like:

a) Diffie– Hellman key trade (DH) is a technique for safely trading cryptographic keys over an open channel. It permits two gatherings that have no earlier learning of each other to mutually build up a common mystery key over an uncertain channel. This key would then be able to be utilized to encode resulting interchanges utilizing a symmetric key figure.

b) RSA (Rivest– Shamir– Adleman) is one of the indispensable open key cryptosystems and is for the most part used for secure data transferral. In such a cryptosystem, the encryption key is open and it is special in connection to the unraveling key which is kept secret (private). The RSA estimation incorporates four phases: key age, key flow, encryption and unscrambling.

c) Elliptic-twist cryptography (ECC) is an approach to manage open key cryptography in light of the arithmetical structure of elliptic twists around restricted fields. ECC requires tinier keys diverged from non-ECC cryptography (in perspective of plain Galois fields) to give parallel security.

d) The YAK is an open key validated key understanding convention, proposed by Feng Hao in 2010. It is viewed as the least complex among the related conventions, including MQV, HMQV, Station-to-Station convention, SSL/TLS and so on. The confirmation depends on open key sets. Similarly as with different conventions, YAK regularly requires a Public Key Infrastructure to convey valid open keys to the imparting parties.

IV. LITERATURE REVIEW

Christian Gehrmann et.al, (2017) proposed in this paper [6], different techniques to protect the distributed IoT (DDoS).They proposed the synchronization and mirror machine based techniques to avoid high availability of network attacks within the system. They do not affect in the real time application as it has high attack resistance quality. The protocol helps to communicate both the IoT state information and state manipulations. Author concluded that given approach provide secure and efficient connection to the slower responses. This solution is very useful when it is required to protect the IoT units from the network attacks but they are not efficient in case of real time applications.

Daeyoung Hyun et.al, (2017) have presented in this paper [7], the issue of distributed denial of service (DDoS) attack that affects the security in the IoT. New techniques and platform raised the new issues for the security. For the security of system new procedures are framed that is programming characterized systems administration and system capacities virtualization. The upside of Software characterized organize (SDN) keeping in mind the end goal to alleviate every one of the effects of DDoS. A corresponding grouping of the techniques are important to picked suitable instrument to alleviate the all the security issues. It also helps the network analyst to choose proper mechanism to show effective results. This given mechanism provides the flexibility to all the packets that are redirected to some direction using SDN. Author proposed these methods to eradicate all the issues related to DDoS attacks in effective and efficient manner. Unique bundles that course through systems were hindered because of examination on worried parcels. Subsequently, creator proposed a technique in view of limit to give the effectiveness with a specific end goal to limit the impacts of DDoS. They likewise created open source codes because of security reasons keeping in mind the end goal to decrease arrange based assaults utilizing SDN.

Lulu Liang et.al, (2016) Have investigated in this paper [8], that like every one of the procedures IoT is likewise utilized as a part of the different fields. Due to widely use it causes a major security issue that leads to huge loss in the data or property. IoT has been seen as the vast area in today's modern world for the development and research. However, there is a major issue in the technology that is lack security mechanism to handle security issues. These mechanisms should be less complex and perform all the computational activities to remit the security problems. Author discussed a major attack in an IoT system that is Denial of Service (DOS) attack. IoT is considered as the target system in which kali linux is used as attack tool. This kali linux tool is used to generate the DoS attack using three different methods. Author explained all the experiments in this paper that shows due to DoS attack, a connection generated between the sensor node and PC. In case of method 1, larger size of the packets is directly proportional to the better execution of the attack. All the comparison shown in the paper with conclusion that method one is superior to method 2 and 3.

Jyoti Deogirikar et.al, (2017) proposed in this paper [9], the fundamental topic currently used widely in the research area that is internet of things. IoT has been seen as the vast area in today's modern world for the development and research. However, there is a major issue in the technology that is lack security mechanism to handle security issues. These mechanisms should be less complex and perform all the computational activities to mitigate the security problems. Before the proper implementations of IoT various attacks were identified. Denial of Service (DDoS) is a major issue that degrades the security in the system. Attacks in the IoT can be avoided by taking some precautions like while dealing with instruments that are difficult to handle. Author concluded that there are various prominent attacks like DDoS that affects the system and devalue its performance by providing access to unauthorized user. They raised all the issued that affects the security system within the network so it is necessary to develop new effective and efficient ways to lessen these issues in future.

Yosef Ashibani, et.al, (2017) this paper proposed [10] a context-aware authentication service for mobile users in Smart Home environments. The services that are designed and implemented provide secure and flexible access to local as well as remote users, as demonstrated by the evaluation results. By combining traditional static authentication measures with a dynamic system utilizing a multitude of additional contexts flexible in their nature, both the security and convenience of a system can be molded to the desires of the homeowner. This system demonstrates how this concept can be applied in a smart home application where these policies can dictate which users can access particular services and when. For future work, this work plans to utilize machine learning algorithms to process the data that is already logged to the database and generate robust user profiles which can dictate access based on usage patterns.

Vaishali Kansal et.al, (2017) Have presented in this paper [11], various threats that violated the network or all the statistics within the system. Nowadays, most active attack is Distributed denial-of-service (DDoS) attack. Writer proposed a technique that mitigates all the affects of DDoS attacks. This technique is based on the threshold parameter and assignment strategy. All the online services are hinder due to the involvement of DDoS. These services are unavailable as the bandwidth and resources in the system are flooded by DDoS attacks. Anyone can access the inside system as it is easier for an insider to access all the system and takes control this is also known as insider attack. When insiders instigate its attack against head proxy, insider is detected by these head proxy as they compare all network parameters. Then the detected insider attack on the proxy that is assigned to handle all the effected clients. Author proposed a moving quarry defense mechanism that differentiates the malicious clients from the innocent clients using attack proxies in order to protect it from DDoS attacks. For the detection of inside attacker an effective algorithm was provided by author that is the concept of load balancing. The main purpose of this is to diminish the number of proxies that exists while increasing attack isolation.

Kubra Kalkan et.al, (2016) Have presented in this paper [12], a filtering-based defense mechanisms has been presented to diminish the distributed denial of service attacks. Nowadays, most active attack is Distributed denial-of-service (DDoS) attack. Author proposed a technique that mitigates all the affects of these attacks. All the online services are hinder due to the involvement of DDoS. These services are unavailable as the bandwidth and resources in the system are flooded by attacks. There are various filtering techniques were observed and mentioned their advantages and disadvantages. A proportional codification of the methods are necessary to chose appropriate mechanism to mitigate the all the security issues. It also helps the network analyst to choose proper mechanism to show effective results. Classification provided by the author will help researchers to identify all the issue embedded in the filtering methods. So that, various mechanism invented by researchers to mitigate the effects of DDoS in internet of things. Author main focused to in this paper was to guide security engineers to aware them with the most suited mechanism to use and filtering mechanisms to deaden the DDoS attacks.

Mert Ozcelik et.al, (2017) proposed in this paper [13], that in recent years major population rely and depended on the internet of things for all kinds of operations and functions. As it is considered as the massive challenge to identify the theft within the network and secure it from attackers. With the increase in size of network system and heterogeneity in the system it becomes a major task to secure a computer network. An infectious attack named “Mirai” also called as botnet seriously affected all the operations of IoT this happens cause by the violations of DDoS attacks. Therefore, author proposed different remedies to minimize these issues like software-defined networking the advantage of Software defined network (SDN) in process to mitigate all the affects of DDoS. Second is fog computing that provide global network supremacy and local services simultaneously. They also proposed a edge oriented detection technique against DDoS in internet of things.

V. CONCLUSION

In this review paper, it is ceased that internet of things is the decentralized type of network due to which security and routing are the major issues which affect its performance. In the extinct years various techniques has been proposed which improve network security. In this review paper various procedures are reviewed in terms of certain parameters.

REFERENCES

[1] R. M. Cardoso, N. Mastelari, and M. F. Bassora, “Internet of Things Architecture in the Context of Intelligent Transportation System – A Case Study Towards a Webbased Application Deployment,” in 22nd International Congress of Mechanical Engineering (COBEM 2013), 2013, pp. 7751–7760.

[2] M. Abomhara and G. M. Køien, “Security and privacy in the internet of things: Current status and open issues,” in Privacy and Security in Mobile Systems (PRISMS), International Conference on. IEEE, 2014, pp. 1–8.

[3] L. M. R. Tarouco, L. M. Bertholdo, L. Z. Granville, L. M. R. Arbiza, F. Carbone, M. Marotta, and J. J. C. de Santanna, “Internet of things in healthcare: Interoperatibility and security issues,” in Communications (ICC), IEEE International Conference on. IEEE, 2012, pp. 6121–6125.

[4] A. Mohan, “Cyber security for personal medical devices internet of things,” in Distributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on. IEEE, 2014, pp. 372–374

[5] S. Ramanauskaite and A. Cenys, “Taxonomy of DoS attacks and their countermeasures,” Cent. Eur. J. Comput. Sci., vol. 1, pp. 355–366, 2011.

[6] Christian Gehrmann and Mohammed Ahmed Abdelraheem, “IoT Protection Through Device to Cloud Synchronization”, IEEE 8th International Conference on Cloud Computing Technology and Science, vol. 4, pp. 1-6, 2016.

[7] Daeyoung Hyun, Jinyoug Kim, Dongjin Hong, and Jaehoon (Paul) Jeong, “SDN-based Network Security Functions for Effective DDoS Attack Mitigation”, 2017 IEEE

[8] Lulu Liang, Kai Zheng, Qiankun Sheng, Xin Huang, “A Denial of Service Attack Method for an IoT System”, 8th International Conference on Information Technology in Medicine and Education, vol. 5, pp. 1-3, 2016.

[9] Jyoti Deogirikar, Amarsinh Vidhate, “Security Attacks inIoT: A Survey”, International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud),vol. 4, pp. 3-6, 2017.

[10] Yosef Ashibani, Dylan Kauling, Qusay H. Mahmoud, “A Context-Aware Authentication Service for Smart Homes,” 2017 14th IEEE Annual Consumer Communications &amp; Networking Conference (CCNC).

[11] Vaishali Kansal, Mayank Dave, “DDoS Attack Isolation using Moving Target Defense”, International Conference on Computing, Communication and Automation (ICCCA2017).

[12] Kubra Kalkan, Gurkan Gur, and Fatih Alagoz, “Filtering-Based Defense Mechanisms against DDoS Attacks: A Survey, IEEE SYSTEMS JOURNAL.

[13] Mert Ozc¸ elik, Niaz Chalabianloo, and Gurkan Gur, “Software-Defined Edge Defense against IoT-Based DDoS”, 2017 IEEE International Conference on Computer and Information Technology.