IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 6, June 2019

An Authentication Process for End to End Delay in the Malicious Network using Alert Correlation

R.Sasikumar[1], R.Ramesh[2]

Department of Computer Science and Engineering, K. Ramakrishnan College of Engineering, Samayapuram, Trichy[1,2]

Abstract: Nowadays Internet of Things devices are rapidly developing to support a great deal of end-end devices (E2E) applications and services. But these services require and reliable device authentication for the security of data. Most of the low-cost devices do not include the security mechanisms. This reduces the reliability of the credentials thus leading to the vulnerability. The are many authentication algorithms for normal devices but extending these algorithms to IoT end devices is a difficult task. In this paper we propose an algorithm for the end to end authentication of End-End devices. We use the algorithm called as Alert Correlation Algorithm for the purpose of the authentication of devices. The algorithm uses the hashing method using alphanumeric keys for the security by using cryptography. If any vulnerable user is detected the algorithm generates the alarm and notifies the user. It also stops the data transfer in the network route till the vulnerable user is removed. We use the cloud tool to store the log file data of each and every successful transaction and detected vulnerability. Our work is providing an extended security to the user's data. Only registered users can transmit data in the channel.

Keywords: Internet of Things (IoT), Cloud, Security, Cryptography, Hashing, Alert Correlation Algorithm

I. INTRODUCTION

Internet of Things is presently turning into the developing innovation wave in the present mechanical world. The greater part of the general population in this day and age utilize wireless communication devices such and cell phones, tablet, workstations, wrist watches, electronics hoes and so forth. These gadgets got an extraordinary favourable position innovation and individuals are becoming acclimated to it. IoT gadgets are progressively intelligent and they lessen human work. Numerous applications like the Smart Lock, Sensor locks use IoT gadgets for the Interaction. As it is building up the security of client's information is likewise an unavoidable need to give. This requirement for information security is expanding step by step as assailants are expanding. There is plenty of algorithms for security in conventional gadgets. [08] User authentication is a significant measure of giving security to information. The authentication algorithms produce several rounds of keys for the client's gadget in order to validate a user/device to give security. Some examples of authentication are email login, windows activation and other product activation etc. [07]Cloud computing is a rising field in innovation which gives storage space and developing applications while in movement and from anyplace by utilizing Internet services. Our work is to give the validation of the end-to-end gadgets in nature.

This work depends on giving end-end confirmation of the IoT gadgets. The conventional authentication mechanisms cannot be implemented on IoT devices due to the following constraints: processing capabilities, memory space, and physical deployment of device, size of the devices. These limitations make to give authentication and security a troublesome assignment in IoT devices. The proposed algorithm gives end-end verification of the gadgets and it produces alert upon the location of vulnerabilities.

II. RELATED WORKS

In this section consists described about, Existing algorithm and Techniques for providing authentication in end to end devices. [1] The paper titled, "A Collaborative PHY-Aided Technique for End-to-End IoT Device Authentication", Here, the Authors proposed an algorithm for secure Authentication and Detection of the intruders, attackers, etc. The key principle is to provide security to the devices and users, by Authentication. In this, alphanumeric key has been providing to each user in random fashion. Based on this unique key user and device has validate. The paper titled [2], "Twenty security considerations for cloud-supported Internet of Things", in this paper, the Authors proposed a mechanism to detect unauthorized entry of attack using the three parameters. Those parameters are user id, password and the secret key. Using above parameters proposed algorithm detects an intruder in the network channel/router. The key is generated based on Hash Algorithm and Alert correlation algorithm to intimate attack.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 6, June 2019

The paper titled [3], "Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A networks", in this paper, provides a better security towards authentication of users. Each user key is stored in the server securely and intrusions are clearly stored with time, date, name of the source user and the name of the destination user. The user or service provider can access this information from anywhere at any time using the cloud tool based on IoT.

III. PROPOSED WORK

In this section described about, Architecture and Techniques used in the proposed paper. proposed work to provide End to End (E2E) authentication of IoT devices when data transmission happened from one device to another device. Each node must be registered with the server when nodes want to communicate with our network devices.[05] During this process, each node has a unique key to log in the network every instance. Every node status is frequently updated by the system in the log directory. In the entire node, information is stored in the database and it can be removed from the database by only authorized device. The node can't log in twice at the same time if an intrusion occurs, then the alarm will automatically generate. Detect generic anomalies rather than deliberate malicious injections, so they are not designed to cope with collusion, this drastically decreases the chances of detection.

3.1 System Architecture

The system architecture is as shown in Figure 1. The system architecture consists of the following four phases. The Set-Up Phase, Packet Transmission Phase, Audit Phase, Detection Phase.

3.1.1 Set-Up Phase(S): Node (n) can join in the network. This phase takes place after route is established, but before any data packets are transmitted over the route. During the set up phase, each node must provide its unique parameters like device id (id), device name (N) to verify the device. This request has been send to server for authentication. Once device has validated, then unique key will be provided to each device in Key Generation phase.

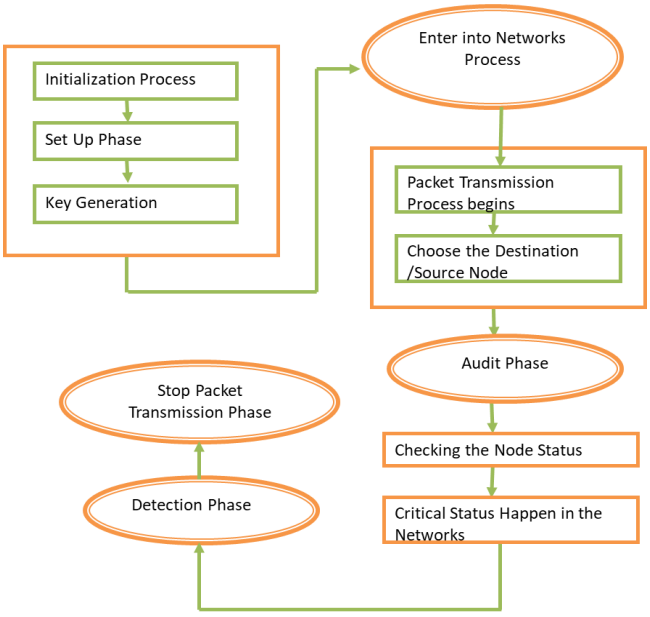

Figure1: System Architecture

Figure 2: Registration Phase

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 6, June 2019

This key generated based on symmetric-key crypto-system. Using this generate key the user enters the credentials (i.e.) his device id and the password as per his convenience and registers with the key in the network. After the registration of the user he can login to the network using the details provided and the secret key given to by the network.

3.1.2 The Packet Transmission Phase:

After completing the setup phase(S), the 'n' enters into the packet transmission phase. Now the device transmits packets to the network server. Before sending out a packet Pi, where i is a sequence number that uniquely identifies Pi, S computes and generates the HLA signatures of ri for node nj, as follows the node has received, and it relays to the next hop on the route. The last hop, i.e., node nK, only forwards Pi to the destination D. The packet transmission takes place between the legal users in the network and if any user is present twice or thrice it is detected as an intrusion and the transmission has refrained to that user till the attackers are removed.

Figure 3: Intrusion Detection

3.1.3 The Audit Phase:

In this phase, without loss of generality, let the sequence number of the packets recorded in the current proof-of-reception database (d). In the above mechanism only guarantees that a node cannot understate its packet loss, i.e., it cannot claim the reception of a packet that it actually did not receive. This instrument can't anticipate a 'n' from excessively expressing its parcel misfortune by asserting that it didn't get a bundle that it really got.

3.1.4 The Attack Detection Phase:

Initially, the server has its own public auditor to verify the entire process. The public auditor (pa) enters the detection phase after receiving and auditing the reply to its challenge from all nodes on PSD. The main tasks of 'pa' include the following: detection of packet loss at each node. In the constructing a packet-loss bitmap for each hop, calculating the autocorrelation function for the packet loss on each node n, and deciding whether malicious behaviour is present with help of Alert Correlation Algorithm.

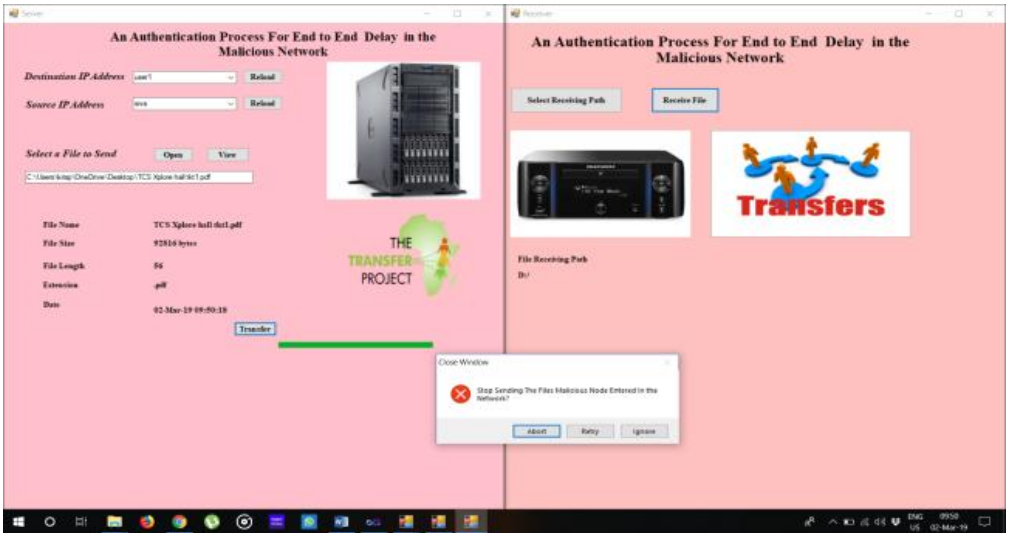

Figure 5: Transmission Refrained due to Intrusion

3.1.5 Algorithm Explanation:

The proposed method use Alert Correlation Algorithm to detect unauthorized access in the node. The algorithm is a system that receives alerts from heterogeneous intrusion detections. This algorithm detects high level of attacks in and reduces the unnecessary false alerts. This algorithm also predicts the state of attack in present and also future state of attack in advance thus reducing the vulnerability to the attacks. The algorithm is classified into three types as similarity, knowledge, statistical based. The first two types require only less context information and it works based on previous attacks and activities. The third type knowledge-based runs completely based upon the meaning of the attacks that have been occurred. Our proposed work uses the simple format of this algorithm to detect intrusion and generate an alarm for the detected anomaly.

IV. CONCLUSION AND FUTURE ENHANCEMENTS

Thus, the proposed system is developed and the system was executed efficiently. Each section has explained based on the out received during implementation. The users can easily register and login to perform data transfer in the network. The network was monitored efficiently and the intrusions are detected if a same user is present in the network. The data transfer is stopped upon the detection of intrusion and thus malicious user is made to logout. Thus, the security was efficiently provided for the devices In future we plan to extend these measures to IoT sensor nodes and provide authentication of Sensor device. Also, this can be extended multiple end devices using the LAN Network.

REFERENCES

[1]. Xianbin Wang, Weiming Shen (2018), “A Collaborative PHY-Aided Technique for End-to-End IoT Device Authentication”, Digital Object Identifier 10.1109/ACCESS.2018.2859781.
[2]. J. Singh, T. Pasquier, J. M. Bacon, H. Ko, and D. Eyers, “Twenty security considerations for cloud-supported Internet of Things," IEEE Internet Things J., vol. 3, no. 3, pp. 269_284, Jul. 2016.
[3]. Mirheidari S.A., Arshad S., Jalili R. (2013) Alert Correlation Algorithms: A Survey and Taxonomy. In: Wang G., Ray I., Feng D., Rajarajan M. (eds) Cyberspace Safety and Security. Lecture Notes in Computer Science, vol 8300. Springer, Cham.
[4]. Gu, G., Cardenas, A.A., Lee, W.: Principled reasoning and practical applications of alert fusion in intrusion detection systems. In: Proceedings of ACM Symposium on Information, Computer and Communications Security, pp. 136–147 (2008).
[5]. X.Wang, P. Hao, and L. Hanzo, ``Physical-layer authentication for wireless security enhancement: Current challenges and future development," IEEE Commun. Mag., vol. 54, no. 6, pp. 152_158, Jun. 2016.
[6]. B.Kiran Bala, A Novel Approach to Generate a Key for Cryptographic Algorithm, Journal of Chemical and Pharmaceutical Sciences, (JCHPS), Special Issue 2: February 2017, Page 229-231.
[7]. D. He and S. Zeadally, ``An analysis of RFID authentication schemes for Internet of Things in healthcare environment using elliptic curve cryptography, "IEEE Internet Things J., vol. 2, no. 1, pp. 72_83, Feb. 2015.
[8]. J. R.Wallrabenstein, ``Practical and secure IoT device authentication using physical unclonable functions," in Proc. IEEE Int. Conf. Future Internet Things Cloud, Aug. 2016, pp. 99_106.
[9]. B.Kiran Bala , J.Lourdu Joanna, Multi Modal Biometrics using Cryptographic Algorithm, European Jour of Academic Essays 1(1): 6-10, 2014.