AN ENCRYPTION-BASED SECURE SDN FRAMEWORK FOR DATA TRANSMISSION IN IOT

[1]Jarapala Parvathi, [2]Devender Nayini

[1]parvathi.cse@gmail.com, [2] devender5c5@gmail.com

[1]Lecturer, Department of CSE, Singareni Collieries Polytechnic, Mancherial, Telangana, India.

[2] Assistant Professor Department of CSE, Balaji Institute of Technology & Science,Warangal, Telangana, India.

Abstract: The Internet of Things (IoT) is a recent trend that extends the boundary of the Internet to include a wide variety of computing devices. Connecting many stand-alone IoT systems through the Internet introduces many challenges, with security being front-and-center since much of the collected information will be exposed to a wide and often unknown audience. The IoT devices required privacy, validation, gets to control, honest keeping in mind the end goal to keep a few attacks. In this paper, a brief is given of the current security challenges on IoT devices and a Software-defined networking (SDN) that can solve problems like resource availability, virtualization and network security by using an encryption algorithm is proposed if any collision occurs in the message transmission.

KEYWORDS: Internet of Things; security; Software-defined networking (SDN), Encryption.

I. INTRODUCTION

Recent developments in many relevant areas, including automation, wireless sensor networks, embedded systems and micro-electromechanical systems (MEMS), has accelerated the evolution of the Internet of Things (IoT) [1]. Currently, IoT applications exist in nearly every field and are playing an increasingly important role in our daily life (e.g., healthcare systems, building and home automation, environmental monitoring, infrastructure management, energy management and transportation systems), which has led to the recent proliferation of IoT systems. According to the Federal Trade Commission (FTC), the number of IoT devices has already outnumbered the number of people in the workplace [3] and the number of wireless devices connected to the Internet of Things will be about 26 billion by 2020 and will greatly outnumber hub devices (smart phones, tablets and PCs).

The Internet of Things is an innovation that is by and by dynamical and reexamining business and society. The greater part of these IoT brilliant devices can't be in homes or telephones, these are in organizations and ventures (e.g. Social insurance). Since these devices are sent into the field, to track and oversee fundamental information, to build the proficiency of work. In this way, security concerns may ascend also. In view of the utilization of IoT devices, security measures at different levels are dealt with. Be that as it may, as the system and information stream is concerned, a safe routing protocol or add a security highlight to routing protocol with least overhead is required. The security issues are likewise that this device once made can't be refreshed, the equipment changes are impossible after the execution it is needed to think before the usage anyway that can roll out improvements in the software field. Let us additionally run over the security in the Authentication and Authorization and here and there likewise in the classification of our information put away. There are numerous framework that is in danger to this security issues, for instance, the home mechanization framework if can change the telephone number that is given in the framework that he can work from home. The portable framework is additionally experiencing numerous issues where there is the issue of protection and the validation.

A portion of the attacks that are confronting by us today are:

1. Distortion: At the moment that the devices in splendid home perform correspondence with the application server, the attacker may accumulate the bundles by changing the coordinating table in the gateway. Regardless of the way that the SSL (secure connection layer) methodology is associated, an attacker can avoid the delivered confirmation. Thus, the attacker can misinterpret the substance of data or may discharge the mystery of data. To anchor the smart home framework from this strike, SSL strategy with proper affirmation instrument should be associated. It is in like manner fundamental to square unapproved devices that may try to get to the splendid home framework.

2. Checking and individual data spillage attack: Wellbeing is one of the crucial purposes of an insightful home. Accordingly, there is an extensive measure of sensors that are used for fire checking, youngster watching and housebreaking, etc. In case these sensors are hacked by an interloper then he can screen the home and access singular information. To avoid this strike, data encryption must be associated with section and sensors or customer affirmation for the acknowledgment of unapproved get together may be associated [4].

II. LITERATURE REVIEW

Framework security generally focuses on general IoT structure to recognize unmistakable security challenges, to design different security structures and to give fitting security rules remembering the true objective to keep up the security of a framework. Structure security basically focuses on general IoT system to recognize various security challenges, to plot unmistakable security frameworks and to give honest to goodness security leads in order to keep up the security of a framework. Application Security works for IoT application to manage security issues according to circumstance necessities. Framework security oversees anchoring the IoT correspondence sort out for correspondence of different IoT contraptions [3]. Information protection and security: A couple of makers of sharp TVs accumulate data about their customers to research their audit affinities so the data assembled by the splendid TVs may have a test for data security in the midst of transmission.

a. Physical Attack: This attack always takes place in the physical layer. The principle of physical attacks is spoofing, listening in, sticking, node replication attack and so on.

b. Sticking: Sticking attacks can be portrayed as the radio flag that meddles the correspondence and endeavoring to hinder inside physical layer. Two type of sticking are Constant sticking impact and discontinuous sticking the sensor not can impart by trading information intermittently but rather not always.

c. Impact: Impact can happen when two imparting nodes trade the information at the same time at a similar recurrence. This kind of attacks diminishes the effectiveness of the system. In this method, the attack can be done by impacting certain bundles amid the transmission. The crash attack is happening on information connect layer.

d. Fatigue: This assumes control over the vitality assets and reductions the productivity. This attack happens on the interface layer of the system [5].

e. Modification of Information: It is a widely recognized attack on arranging layer. The altered data is identified with routing choice. The data is antagonistically affected by adjusting or replaying the message contents. IOT is defenseless to listening in, consequently, the adversary can without much of a stretch to examine the transmission and can alter or intrude on the activity. Because of this alteration, false data is transmitted to conveying nodes. These attacks make new ways of routing and method of delivering false messages, repulse or draw in the rush hour gridlock of the system, increment or lessening the routing ways, abbreviate or extend the idleness time.

f. Encryption Algorithms. It was divided in two kinds of symmetric cryptography and unbalanced cryptography. While Albeit open key encryption is more vigorous and gives preferred security over mystery key encryption, it isn't utilized as a part of IOTs specifically due to its moderate execution and prerequisite of more memory [6]. Symmetric cryptography calculations are talked about essentially in two classes as square and bit stream encryption calculations. Square encryption calculations take settled length squares of information to be encoded into the encryption work and produce scrambled information hinder with a similar length. For instance, for these calculations, AES, DES, Skipjack, RC5 etc are given. In any case, bit stream encryption calculations take information as a gushing arrangement of bits.

III. PROPOSED SYSTEM

The Proposed System Architecture is shown in below Figure (1) it describes the encryption based security for a message in an IoT environment using SDN Software.

A. SDN ARCHITECTURE

The basic objectives of a secure communications network are confidentiality, Privacy, integrity, availability of information, Approval, control of access, Policy implementation and abrogation. In addition to supporting a network secured from malware attacks or accidental damage, security authorities must secure the data, the network properties and the communication transactions over the net. The modifications to the network architecture presented by SDN should ensure that the network security is constant. The crucial feature of SDN is the split-up of the forwarding along with control layers. The functionality of forwarding, comprising the logic as well as tables for selecting exactly accomplishes with inward packets and features like identical or dissimilar networks. The significant movements attained by means of the forwarding level can be well-defined by the method with incoming packets. It consists of consuming, sending, droplet or repetition of an arriving packet. If data packet released owing to specific transmission issue to the control server, do the retransmission and controls “data packet loss”.

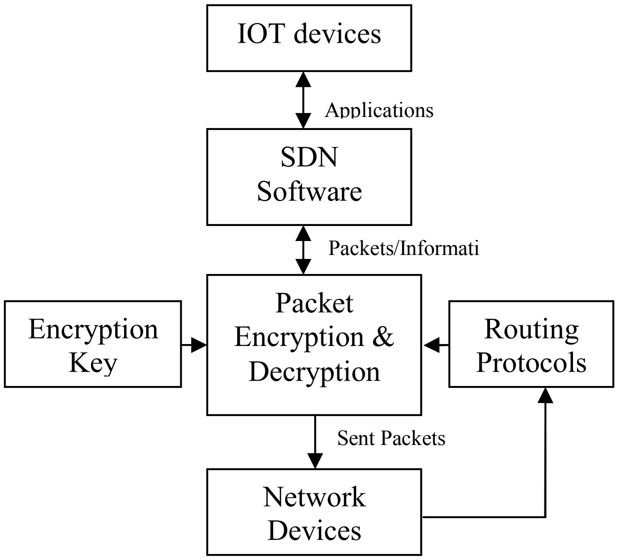

Fig. 1: PROPOSED SYSTEM ARCHITECTURE

B. PACKET ENCRYPTION AND DECRYPTION ALGORITHM

The answer for a security issue in IOT routing is to utilize straightforward protocol with a capacity of scrambling information with the private key. For this adjustment should be done in the existing bundle structure. This procedure can be used with any routing protocol as it just includes a change to the client information part. These keys are likewise put away in each base node alongside the one of a kind ID of the bit. All the client information in messages scrambled utilizing an arbitrarily chosen key from the great encryption key. First On the off chance that the client data is to be encoded then an uncommon 7-bit design is additionally scrambled utilizing a similar key. This example can be each of the 1s (111111) or every one of the 0s (0000000) or any blend of 0s. This little example is used to limit information unscrambling at the base station as decoding huge information will take all the more preparing time and figuring powers.

Encryption Procedure

```
1. let good keys = {x>0|x belong to unique secrete keys}
2. let bit pattern = unique 7 bit pattern
3. secrete key = random (good key)
4.encrypted_pattern=encrypt(bit pattern, secrete key) so that length(encrypted pattern)=7 and decrypt(encrypted pattern, secrete key) = bit pattern while decrypt(encrypted pattern, wrong key) !=bit pattern

5. encypted_data = encrypt (data, secrete_key)
6. make and send packet
7. Exit
```

Decryption Procedure

```
1. let good_keys = {x>0|x belong to unique secrete keys}
2. let bit_pattern = unique 7 bit pattern
3. secrete_key= get_next_secrete_key(unique ID of Sender)
4. decrypted_pattern = decrypt(encypted_pattern,secrete_key)
5. if decypted_pattern = null then drop Packet and Exit
6. if decypted_pattern = bit_pattern then go to step 7 else go to step 4
7. data = decrypt (encypted_pattern, secrete_key) process data
```

The information is sent utilizing typical routing strategies. The base station first checks whether the received message is scrambled or not then finds on the main piece of client information. In Encrypted bundle, the following 7-bit design is unscrambled utilizing all the keys and the decoded string is coordinated against putting away piece design and a match are discovered at that point by utilizing coming about mystery key whatever is left of the messages are decoded.

IV. RESULTS

This section describes about the results that are obtained by implementing the proposed algorithm. The suggested technique offers safe communication concerning clients along with the server. If any collision or drop occurs during the transmission, it can be again transmitted to revoke. However, the existing scheme cannot offer retransmission. The Performance metrics such as Packet Delivery Ratio (PDR), End-to-End delay, energy efficiency, security and throughput is given in Figure (2) for the suggested technique using Network- Simulator-2 environment compared to WSN (Wireless Sensor Network) Architecture .

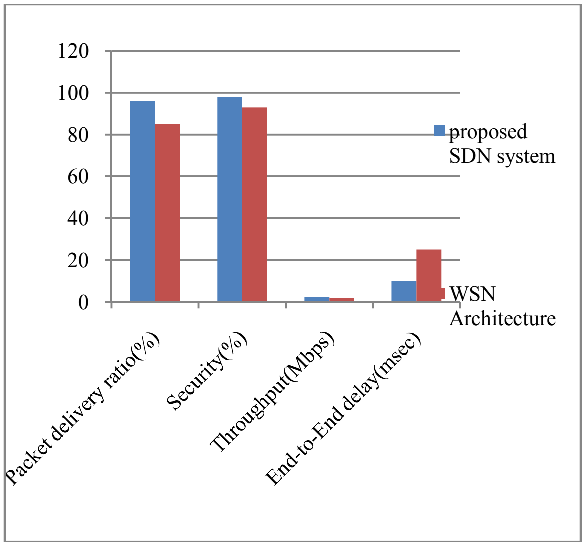

Fig. 2: PERFORMANCE COMPARISON

V. CONCLUSION

The IoT security has been an essential test because of its unmonitored arrangement of nature and its innate assets restriction. Because of restricted assets of sensor nodes, the security in IoT has turned out to be harder to actualize when contrasted with other conventional systems. Different methods had sent to determine the security issues. For this reason, an Encryption-Based Secure SDN Framework for Data Transmission in IoT is proposed in this paper. The calculation exhibited here is a stage toward taking care of this security issue with basic salt based encryption. A suitable solution outline of the IoT security is also planned to overcome the security concerns in IoT framework. Finally, the issues along with challenges to the IoT security were deliberated with the security of 96.2%.

VI. REFERENCES

[1] A. Tewari and B. B. Gupta, "A robust anonymity preserving authentication protocol for IoT devices", *Consumer Electronics (ICCE) 2018 IEEE International Conference on*, pp. 1-5, 2018,

[2] Nitti, M.; Pilloni, V.; Colistra, G.; Atzori, L. The Virtual Object as a Major Element of the Internet of Things: A Survey. IEEE Commun. Surv. Tutor. 2016, 18, 1228–1240.

[3] Blazquez, A.; Tsiatsis, V.; Vandikas, K. Performance Evaluation of OpenID Connect for an IoT Information Marketplace. In Proceedings of the 81st IEEE Vehicular Technology Conference (VTC Spring), Glasgow, UK, 11–14 May 2015; pp. 1–6.

[4] S. Raza, H. Shafagh, K. Hewage, R. Hummer, and T. Voigt, "Lithe: Lightweight secure CoAP for the Internet of Things, "IEEE Sensors J., vol. 13, no. 10, pp. 3711–3720, Oct. 2013.

[5] R. Hummer, J. H. Ziegeldorf, H. Shafagh, S. Raza, and K. Wehrle, "Towards viable certificate-based authentication for the Internet of Things, " in Proc. 2nd ACM Workshop Hot Topics Wireless Security. Privacy, 2013, pp. 37–42.

[6] Federal Trade Commission. Internet of Things—Privacy and Security in a Connected World; FTC: Seattle, WA, USA, 2013.

[7] Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020; Gartner Inc.: Stamford, CT, USA, 2013.

[8] E. Rescorla and N. Modadugu, Datagram Transport Layer Security, document IETF RFC 6347, Jan. 2012.

[9] J. Hui and P. Thubert, Compression Format for IPv6 Datagrams Over IEEE 802.15.4-Based Networks, document IETF RFC 6282, Sep. 2011.

[10] W. Stallings, Cryptography and Network Security: Principles and Practice: Prentice Hall Press, 2010.

Jarapala Parvathi is currently working as a Lecturer in the Department of Computer Science & Engineering, Singareni Collieries Polytechnic, Mancherial, Telangana, India. She is having 10 years of experience in teaching and her area of interest includes Network Security, IOT, Cloud Computing and Machine Learning etc.

Nayini Devender has 3+ years experience as Assistant Professor in the Department of Computer Science & Engineering, BITS, Warangal, India and he is a life member of ISTE. He has published more than 3 research papers. His area of research includes Internet of Things (IoT), image processing etc