ISSN XXXX XXXX © 2019 IJESC

Research Article Volume 9 Issue No.4

Verifying IOT with Software Defined Networking

Shimona Balla[1], Priyanka Verma[2]
B. Tech Student[1, 2]
Department of Computer Science
SRM University, Chennai, India

Abstract:
With the developing Internet of Things (IoT) innovation, there is an exponential development, multifaceted nature in network and overseeing of heterogeneous gadgets to the web. Security being the real worry of such complex heterogeneous systems and their differing access conventions is a genuine test. SDN is a shrewd systems administration worldview that manages these situations by breaking vertical mix, isolating the system's control rationale from the basic switches and switches, advancing centralization of system control and acquainting the capacity with program the system. The partition of concerns presented between the meaning of system arrangements, their usage in exchanging equipment and sending traffic is critical to wanted adaptability.

Keywords: Programming characterized organizing, SDN, Network virtualization, IOT.

I.INTRODUCTION

IoT represents a system which consists of things in the real world and sensors attached to or combined to these things connected to the internet via wired and wireless network structure.By the IoT objects recognize themselves and obtain intelligence behavior by making relative decisions and communicating information among themselves. Various IoT applications include smart cities, smart home and buildings, smart health, smart agriculture etc. SDN is emerging network architecture where control is decoupled from forwarding and is directly programmable. It provides more efficient configuration, better performance and higher flexibility to accommodate innovative network designs. In this project we have merged IoT with SDN to enhance the network security of IoT and make the network easily programmable.

II.RELATED WORK

Each device of IOT connected in a network follows different accessing and security mechanism with a drawback of making the network more complex to manage. Scalability posing a major challenge in IOT for providing communication environment for billions of devices for interaction with a drawback of poor communication between the IOT devices connected in the network. Limited resource availability as they become vulnerable to attackers. Minimization of the communication and computation overhead providing inefficiency in the network. Poor transportation of information among the IOT devices leads to ineffective communication. No integrity in the network of IOT devices resulting in no effective updates and violation of the network

III. LITERATURE SURVEY

TITLE: Securing IoT with SDN.
AUTHOR: Kubra Kalkan
YEAR: 2016.
DESCRIPTION:
Over the most recent few years Software Defined Network (SDN) has appeared which enables arrange administrators with greater adaptability to oversee and program their system. This kind of system comprehends the restriction of inheritance systems. Information plane and control planes are isolated from one another accordingly information plane gadgets straight forward go about as a parcel sending gadget and leaving the basic leadership part to a brought together framework called controller. In spite of the fact that it has a ton of focal points, still security of SDN is an open issue.

TITLE: Securing IoT devices using SDN and Edge Computing
AUTHOR: Christian Esteve Rothenberg,
YEAR: 2015.
DESCRIPTION:
In the current mechanical point of view, we are seeing an enormous increment in the association of heterogeneous gadgets and controlling them remotely. Since the gadgets which are being associated would be straightforwardly controlling human life, the security of these gadgets ends up central. There are diverse strategies for giving security to a system accessible today however none is trustworthy. SDN being a clever systems administration worldview which can quickly and consequently reconfigure arrange gadgets reroute traffic and apply validation and access tenets can open up a path for better security and access control instruments. In this paper, an endeavor has been made to devise a technique for giving security to IoT utilizing SDN (Software Defined Network) and Edge Computing.

TITLE: Enabling cooperative IoT security via SDN**AUTHOR:** Steve Uhlig
YEAR: 2017
DESCRIPTION:
Web of Things (IoT) is turning into an undeniably alluring focus for cybercriminals. We see that numerous assaults to IoTs are propelled in a conniving manner, for example, animal power hacking usernames and passwords, to focus at a specific injured individual. To this end, we propose to use Software Defined Networks (SDN) to empower helpful security for heritage IP-based IoT gadgets. SDN decouples control plane and information plane, and can help connect the learning partitioned

between the application and system layers. In this paper, we examine the IoT security issues and difficulties, and present a SDN-based engineering to empower IoT security in an agreeable way. Moreover, we executed a stage that can rapidly impart the assaulting data to peer controllers and square the assaults. We completed our trials in both virtual and physical SDN situations with OpenFlow switches. Our assessment results demonstrate that the two conditions can scale well to deal with assaults; however equipment usage is significantly more effective than a virtual one.

TITLE: Improvement in IOT based on Software-Defined Networking.
AUTHOR: Vandana C.P
YEAR: 2017.
DESCRIPTION:
The making vitality for the sharp gadget/home/city has acknowledged becoming indisputable nature of Internet of Things (IoT) sending. Be that as it may, because of the open and heterogeneous nature of IoT systems, there are different difficulties to convey an IoT arrange, among which security and versatility are the main two to be tended to. To improve the security and adaptability for IoT systems, we propose a Software-Defined Virtual Private Network (SD-VPN) arrangement, in which each IoT application is distributed with its own overlay VPN. The SD-VPN arrangement can improve the security of an IoT organize by isolating the VPN traffic and using administration binding. In the meantime, it additionally improves the adaptability by its overlay VPN nature and the VxLAN innovation.

TITLE: Software- Defined Networking: A Comprehensive Survey
AUTHOR: M.V. Ramos
YEAR: 2014.
DESCRIPTION:
The Internet has prompted the formation of an advanced society, where (nearly) everything is associated and is available from anyplace. Be that as it may, in spite of their boundless reception, conventional IP systems are perplexing and exceptionally difficult to oversee. It is both hard to design the system as indicated by predefined arrangements, and to reconfigure it to react to shortcomings, burden, and changes. To make matters considerably increasingly troublesome, current systems are additionally vertically incorporated: the control and information planes are packaged together. Programming characterized organizing (SDN) is a rising worldview that guarantees to change this situation, by breaking vertical combination, isolating the system's control rationale from the fundamental switches and switches, advancing (intelligent) centralization of system control, and acquainting the capacity with program the system.

IV. EXSISTING SYSTEM

Each device of IoT connected in a network follows different accessing and security mechanism. Scalability posing a major challenge in IoT for providing communication environment for billions of devices for interaction. Limited system's availability. Minimization of the communication and computation overhead.

V. PROPOSED SYSTEM

In this paper, two different models are being proposed for securing the IOT devices. Basically, the entire range of IoT devices can be divided into two segments depending upon how they get connected to the Internet

i. Using network access end point devices (e.g. Wi- Fi routers and switches) which further connect to the Internet using their respective ISPs
ii. ii. Using Cellular Mobile Operators i.e. 4G and 5G networks.

VI. MODULE DESCRIPTION

1. Hybrid Encryption algorithm
2. Merging IOT with SDN

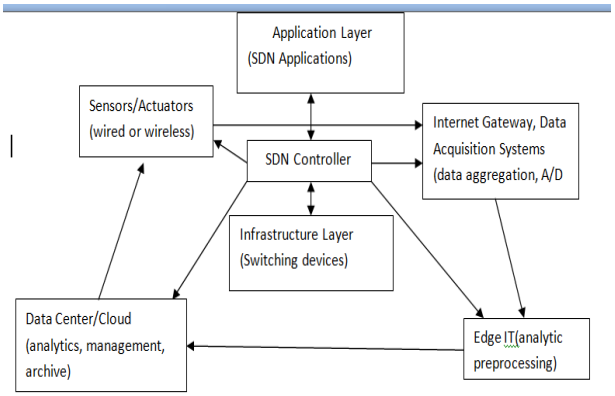
HYBRID ENCRYPTION ALGORITHM

It is used to preserve information integrity, confidentiality and being non-repudiation to secure the exchange of data for IOT. It has special features of encryption and decryption in terms of speed in building the keys. It can also improve the internet security using digital signature. Steps of smart home cryptography. The user has the public key that is generated by the symmetric encryption. New messages for encryption are sent by asymmetric algorithm by the public key. Then the message is encrypted by asymmetric encryption algorithm and will be sent to the receptor in the internet environment. Receptor uses a private key and that even the user or sender is unaware of it.

MERGING IOT WITH SDN

Customary security instruments like Firewalling, Intrusion Detection and Prevention Systems are conveyed at the Internet edge. Those mechanisms are used to protect the network from external attacks. Such mechanisms are no longer enough to secure the next generation Internet. The borderless architecture of the IOT raises additional concerns over network access control and software verification.

VII. SYSTEM ARCHITECTURE



CHALLENGES

- The two major challenges of the IOT devices which are heterogeneity and scalability that are the hindrance in today's existing system is met successfully through SDN controller that manages the heterogeneous network and incoming and outgoing of the packets.

- When it comes to scalability that poses a problem in the communication environment of billions of devices for

interacting is resolved through the dynamic and agile nature of the SDN paradigm.

- Host-based intrusion detection is used instead of network-based detection which decreases the volume of traffic that needs to be monitored,hence minimizing the communication and computation overhead

VIII. CONCLUSION

We introduce a trustworthy, cooperative and scalable architecture to enable IoT security among multiple networks. The architecture is powered by SDN technologies, where the controller application can take input about malicious activities from its end systems and translate their requirements to the network-level flow rules to stop attacks quickly. The architecture can not only benefit the victims under attacks, but any other potential targets in the networks. In addition, we solved the trust problem through double checking the traces of the malicious traffic. Meanwhile, we measured the time spent in each phase in both virtual and real environments. The results show that the overall hardware implementation outperforms the same implementation in a virtual environment.

IX.REFERENCES

[1]. IDC Predictions 2013: Competing on the third Platform, IDC, Framingham, MA, USA, Nov. 2012, White Paper. [Online]. Available: http://www.idc.com/ask about/ Predictions 13/ downloadable/238044.pdf

[2]. P.Mell and T. Grance, "The NIST importance of conveyed processing (draft)," NIST Special Publication, vol. 800-145, p. 7, 2011.

[3]. J. Gantz and D. Reinsel, "Removing a motivating force from tumult," IDC, Framingham, MA, USA, White Paper, Jun. 2011. [Online]. Open: http://www.emc.com/ensure/agent reports/idc-isolating valuefrom-uproar ar.pdf

[4]. J. Manyika et al., "Tremendous data: The accompanying edges for progression, contention, and effectiveness," McKinsey Global Inst., Mumbai, India, pp. 1– 137, 2011.

[5]. P. Cesar and D. Geerts, "Past, present, and possible destiny of social TV: An order," in Proc. IEEE CCNC, 2011, pp. 347–351.

[6]. Y. Jin, X. Liu, Y. Wen, and J. Cai, "Between screen joint effort for session affirmation and trade subject to cloud driven media mastermind," in Proc. IEEE ISCAS, 2013, pp. 877– 880.

[7]. Y. Jin, Y. Wen, G. Shi, G. Wang, and A. Vasilakos, "CoDaaS: A test cloud-driven substance transport arrange for user generated substance," in Proc. Int. Conf. Comput. Netw. Commun., 2012, pp. 934– 938.

[8]. J. Senior part and S. Ghemawat, "MapReduce: Simplified data getting ready on broad gatherings," Commun. ACM, vol. 51, no. 1, pp. 107– 113, Jan. 2008.

[9]. "Cisco visual frameworks organization record: Global adaptable data traffic gauge update, 2013– 2018," San Jose, CA, USA, White Paper, Feb. 2014.

[10]. Facebook Timeline. [Online]. Available: http:// news room.fb. com/Timeline

[11]. "SourceFire Inc." [Online]. Available: http:// www. snort. org

[12]. Hu H, Han W, Ahn J, Zhao Z. Flowguard: Building solid firewalls for programming described frameworks. Third Workshop on Hot Topics in Software Defined Networking. 2014. p. 97-102.