iJRASET

International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 Issue: VII Month of publication: July 2022

DOI: https://doi.org/10.22214/ijraset.2022.45417

A Survey on New Security improvement in Internet of Things utilized by Software Defined Networking (SDN)

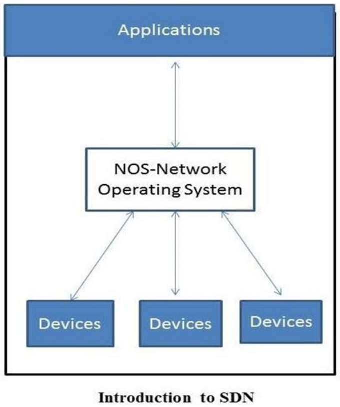
Mr. Manikandan B[1], Mr. Murugan.K[2]
[1]*Assistant Professor, Department of Information Technology,Hindusthan Institute of Technology Coimbatore*
[2]*Assistant Professor, Department of Computer Science and Engineering, Hindusthan Institute of Technology Coimbatore*

Abstract: IoT Security is that the realm of endeavor concerned with safeguarding connected devices and networks with within the internet of things (IoT). IoT is a forthcoming innovation that produces utilization of web to control/screen electronic, mechanical gadgets, automobiles and other physical gadgets associated by means of networking. Reliability of such intricate diversified networks and their access protocols is additionally a real challenge which leads to security risk. Combination of Software Defined Networking with IoT can lead the way for better security and access control mechanisms. SDN could even be an intelligent networking paradigm which reveals vast opportunities to manage and secure IoT. The SDN approach focuses on the programmability for all network elements. Thus SDN based IoT architecture is often employed to workout security framework.

Keywords: SDN, IoT

I. INTRODUCTION

In today's world of dynamic requirements, the network state changes continuously and gets updated as per the changing need of the purchaser. Network administrators and operators must adjust network configuration accordingly. Basically, IoT is a technology which aims towards connecting physical objects, devices through the online. Thephysical devices are often connected to the online through Wi-Fi (802.11),3G, 4G network, LTE network and Bluetooth. because the voluminous devices are connected to the network, the complexity of connecting these countless devices increases. Also, the networks should find these devices and connect with them then route the traffic and make the inspiration about how each individual device are visiting used followed by monitoring of those connections and thus the data which is able to generated by them. Thus tolimit the complexity level, usage of SDN becomes essential. As a single point, traditional routers and switches have control over the decisions related to traffic management and actual mechanism for routing traffic to destinations. Due to this single point of control, the devices become slow, expensive, inflexible, non-scalable and sticky. Network operators employ various tools and mechanisms to reconfigure these network parameters as and when required. This results in configuration errors. Software Defined Networking was proposed to disentangle these issues which regular network control standards confronted. SDN aids in discovering and connecting with these devices and so routing their traffic. Differentiation thereto with one router we'd have to composethousand lines of code to achieve this yet with SDN it ought to be taken care of with barely any mouse clicks.



Introduction to SDN

Fig 1: SDN

Software defined networking is a rising innovation and ends up being promising for future organizations. Fig 1 shows the SDN architecture. It uses Open Flow protocol for its implementation [10].Open flow is a communication protocol that provides access to the path through which data packets are transported through a switch or router over the network. Open Flow is the key component to understand SDN and a large number of research works are in favor of SDN / Open Flow are still emerging [12] [13] [14].

Inside the standard strategies for operation for example setup is done gadget by gadget or framework by-framework utilizing manual strategies and just can't scale at the speed required today. Thus automation via network programmability is a savior through which network operations are carried out without wearing out specialists. Along these lines, we'll state that software defined networking isn't just useful for networks yet in addition for business. SDN permits us to boost the assurance, execution while keeping up with consistently changing business needs. As SDN has the ability to adapt up powerfully to the changing client needs or the new traffic designs, security incidents and strategy changes, it will empower IoTsituations to convey on their guarantee.

II. MOTIVATION

Programming characterized networks were made in lightof requests from enormous server farms that discovered issues tending to eccentric traffic patterns. These traffic patterns would cause exceptionally high requests for specificassets that couldn't meet with existing framework. In this way, there are two decisions either proportional the organization framework to fulfill the pinnacles which are pricey or to shape an organization which can reconfigure itself naturally to handle with those pinnacles and channel the assets to fulfill the reasonable requests.

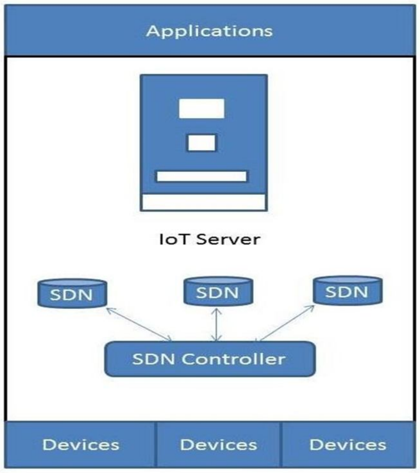


Fig 2: SDN Controller

A. *Software Defined Networking Architecture*

Fig 2 shows the SDN controller in which both the controland information planes are decoupled to have just one unified controller. A programmable interface is given to the isolated control plane having intelligence added to them. Software Defined networks are dynamic and tough, dealing with the significant time requests of IoT.

B. *SDN Controller Features*

1) *Network Programmability:* Because the SDN controllers are programmed it's conceivable to utilize the unpretentious channels to the packets and control the active traffic.
2) *Scalability:* Since the SDN manages variety of networks, SDN controller communicates with the changing networks and gadgets and also number of devices is added ortaken out to the network without influencing its performance.
3) *Centralized Monitoring:* SDN controller empowers the organization with the end-to-end network flow visibility. A SDN controller utilizes the Open Flow information to recognize the issue on a given stream and changes the tail ofthe stream that it takes.
4) *Visualization:* SDN controller gives representation of the various virtual networks that run on physical network. Controller permits the organization to see the outcome of both the physical and virtual network point of view to ask thedefinite data.
5) *Performance:* SDN controller pre-populates the stream tables to its greatest conceivable degree and has greatprocessing and I/O capacity that guarantees unified controller.

III. LITERATURE SURVEY

A. Use of Flood Guard

The work discussed in [1] centers around the responsive controllers and ensuing security dangers against them. A protection structure for SDN networks called flood monitor which is adaptable, productive, lightweight and convention autonomous is proposed to foretell data-to-control plane saturation. Flood monitor system uses proactive flow rule analysis and proactive movement for forestalling data-to- control plane saturation attack. Effect on data transmission under various assault rates with and without flood watch is assessed.

B. SPHINX - controller agnostictool

This tool [2] exploits the threats dependent on the data that open flow messages originating from switches. After confirmation of these messages, custom algorithms are utilized to refresh the networks so that controllers can use it for processing. The flow graphs are used to recognize the security dangers on configuration and information plane by forwarding it within software-defined-networks. SPHINX steadily refreshes the flow graph and recognizes the attacks progressively in real time that some controllers are subject to.

C. SDN for Network Security

This work[3] explains the highlights of software-defined-networks like unique stream control, network wide perceivability with unified control, network programmabilityand improved information plane. Furthermore to those highlights, how network security profits by these previously mentioned highlights is represented with examples. Subsequently top to bottom examination is done during this paper on how software defined networking can carry advantages to security outlined with state-of-art research in related areas.

The paper [4] presents the capacities, organization, applications and furthermore the difficulties confronted giving the more extensive perspective on the idea of adopting Software Designed network for enhancing security by utilizing SDN. Also insights about various programmable networks and the protocols such as OpenFlow, XMPP, OnePk,etc that are adopted by the networks are discussed.

D. Security Challenges in IoT

The review[15] discusses the current situation of IoT with the assurance challenges like identification of object, protection and respectability, verification and approval and malware in IoT. Software defined network idea along with IoT design is examined. Additionally, the wellbeing component upheld the ideas of segment controller and gateway controllers are featured.

IV. PROPOSED ARCHITECTURE

The SDN is an emerging architecture that is dynamic, reasonable savvy and versatile creation. It's a way to deal with computer networking that license network executive to automatically instate, control change and oversee network behavior progressively through open interface and deliberation of the lower level functionality. To frame IoT possible, a reliable adaptation to the common protocols usedin the networking environment of IoT should be built.

The role of IP for the web is critical and is proposed in light of the fact that the answer for IoT, particularly with theprogression of IPv6. This approach has a lot of difficulties and burdens related with heterogeneity of the gadgets and networks engaged with IoT. These objects and their protocols follow explicit plans to satisfy explicit client targets.

Attempting to suit these assorted varieties of the objects into a standard particular protocol is certifiably not a respectable alternative. On the contrary, the Software defined networking approach centers around programmability of all networking components.

A significant issue with respect to SDN security is that virtualizing each part of the network infrastructure increases your attack footprint. The SDN controller generally the primary objective for assailants since it's the main issue for choice in an incredibly network and an essential issue of disappointment.

Because of the programmability highlights of SDN, computer specialists can introduce security applications on the controller’s northbound interface to open up better approaches to utilize security to a network.

SDN make easier to audit network usage, SDN improve policy enforcement through security aspects.

V. CONCLUSION

In this paper, we discussed a survey on new security improvement in IoT supported on Software defined networking. These applications have provided a replacement platform to the voluminous of devices and folks connected over internet. Programmatically initialize, control, change and manage network behavior dynamically. Innovation in SDN technology can drive the IoT platform forward. Stronger Security should provide to devices, in order that theinformation protected.

The survey discussed on this paper provides an agile answer on how improve the IoT security within Software- defined networks.

REFERENCES

[1] Haopei Wang,Lei Xu, Guofei Gu, " FloodGuard: A DoS Attack Prevention Extension in Software-Defined Networks", 2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, pp 239-250

[2] Mohan Dhawan, Rishabh Poddar, Kshiteej Mahajan, and Vijay Mann,"SPHINX: Detecting Security Attacks in SoftwareDefined Networks" NDSS '15, 8-11 February 2015

[3] Seungwon Shin,Lei Xu, Sungmin Hong, Guofei Gu, "Enhancing Network Security through Software Defined Networking (SDN)", 2016 25th International Conference on Computer Communication andNetworks (ICCCN).

[4] Shiva Rowshanrad , Sahar Namvarasl, Vajihe Abdi, Maryam Hajizadeh, Manijeh Keshtgary, "A survey on SDN, the future ofnetwoking", Journal of advanced computer science and technology, 2014, pp 232-248

[5] H. Huang, J. Zhu, and L. Zhang, "An sdn based management framework for iot devices," in Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014). 25th IET. IET, 2013, pp. 175–179.

[6] Muhammad H. Razaa, Shyamala C. Sivakumarb, Ali Nafarieha, Bill Robertsona, "A Comparison of Software defined network(SDN) Implementation Strategies" , Procedia Computer Science 32 (2014) 1050 – 1055

[7] Ola Salman Imad Elhajj Ayman Kayssi Ali Chehab, "SDNControllers: A Comparative study", Proceedings of the 18th Mediterranean Electrotechnical ConferenceMELECON 2016, Limassol, Cyprus, 18-20 April 2016.

[8] Y. Jararweh, M. Al-Ayyoub, A. Darabseh, E. Benkhelifa, M. Vouk, and R.Andy,"Sdiot:a software defined based internet of things frame work," Journal of Ambient Intelligence and Humanized Computing, 2015.

[9] B. Eleonora, "The internet of things vision: key features, applicationsand open issues," Computer Communications, 2014 - Elsevier, 2014.

[10] R. S. Braga, E. Mota, and A. Passito. Lightweight DDoS Flooding Attack Detection Using NOX/Open Flow. In Proceedings of the35th Annual IEEE Conference on Local Computer Networks, LCN, 2010.

[11] Ankur Nayak, Alex Reimers, Nick Feamster, and Russ Clark, "Resonance: Dynamic Access Control for Enterprise Networks." In Proceedings of WREN, 2009.

[12] Sungmin Hong, Robert Baykov, Lei Xu, Srinath Nadimpalli, and Guofei Gu. "Towards SDN-Defined Programmable BYOD (Bring Your Own Device) Security." In NDSS'16, 2016.

[13] Bose I, Pal R, "Auto-ID: managing anything, anywhere, anytime inthe supply chain", Communications of the ACM, vol. 48, no. 8, 2005, pp 100-106.

[14] Eun Joo Kim, Jong Arm Jun, Nae-Soo Kim, " A Packet scheduling Strategy for Heterogeneous Traffic of Internet of Things".

[15] Vandana C.P, "Security improvement in IoT based on Software defined networking" , International Journal of Science, Engineering and Technology Research (IJSETR), Volume 5, Issue 1, January 2016, ISSN:2278-7798