International Journal of Future Generation Communication and Networking
Vol. 13, No. 3s, (2020), pp. 1658–1662

Blockchain based security and resource management models for SDN

Karan Shingare
UG student
Department of Computer Engineering

Mr.P.S.Hanwate
Assistant Professor
Department of Computer Engineering

NBN SINHGAD SCHOOL OF ENGINEERING, AMBEGAON (BK), PUNE.

Abstract

Security, at present, is one of the major concerns in Software Defined Networks (SDN). Resources sharing in SDN can be made more secure against non-trusting members in SDN by the implementation of blockchain technology. It forces the members to trust and creates a secure private network which then increases the reliability of the system. This paper focuses on preventing the system from being tampered with the integrity of the system, which triggers a variety of attacks, by implementing blockchain technology, which provides its immutable performance to the system and a decentralized resource providence and authentication system to the members of the SDN system. The resource management model provides a distributed authentication mechanism that alleviates the problem of being vulnerable at a single point when using the traditional SDN way of getting authenticated through a single point. Also, each node in the SDN system acts as a blockchain node and the list of nodes or devices in the SDN system is distributed among the devices which then can help authenticate any new connection, detecting the malicious user in the system and helps increase the system scale while maintaining the records of authentications of services as a transaction log.

Keywords □ □ *Software Defined Network, Blockchain, network security*

I. INTRODUCTION

Blockchain has been a topic of interest in many sectors like government, finance, health-care and industry, for its unmatched level of security and reliability. Blockchain has a decentralized nature hence the need for monitoring the transactions by any third parties or intermediates is not needed at all and the system can work independently. Blockchain forces the trust among its users who share a common variable and this enforced trust can be very helpful while dealing with transactions in an untrustworthy environment. With Blockchain heavy encryption and cryptography in SDN for security can be implemented[3 4].

SDN has a central control system which can be its greatest weak spot in dealing with external attacks. Especially when scaling the network and adding new devices or end users to the network, the system can be vulnerable to attacks by unauthorized or malicious users being added to the system. In such scenarios, blockchain technology can help reduce the risk by providing its very own properties to the network like immutability and forced trust.

In this paper, we design a method to fuse blockchain technology with SDN to secure it.

This paper is divided into five sections, section II looks into the background of SDN and blockchain technology. Then section III, the core of the paper, where the design of the proposed model is explained in detail. Lastly, section finishes off the paper by discussing the conclusion.

ISSN: 2233-7857 IJFGCN

II. BACKGROUND

In this section, we briefly describe the basics of blockchain and SDN.

A. Blockchain

Blockchain is a truly revolutionary technology. Sometimes referred to as Distributed Ledger System, as it is also defined as a decentralized, distributed ledger system that stores the transactions related to digital asses. There are various reasons to use blockchain for its properties, but simply according to MIT technology review, the whole point is using a blockchain is to let people- in particular, people who don't trust one other- share a valuable data in a secure, non-temperable way. It has two major parts- block and node, node is any networking device (mostly computer or laptop)which acts as a small server and stores block, which is the block that contains three elements - data, nonce- a 32-bit whole number which is generated randomly when any block is created and a 256-bit hash wedded with a nonce.

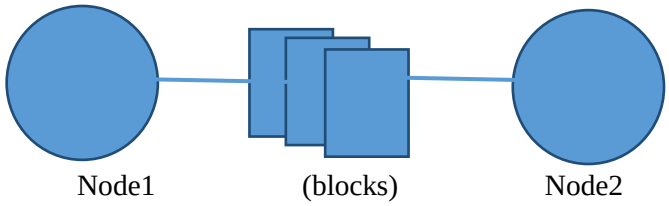

Fig. 1. Blocks and nodes in a blockchain

It does not have any central storage system, and all the transactions are stored at the end-user. Each user has the same copy of the ledger, and each user keeps on updating its copy hence ensuring complete agreement from all users. Although being a decentralized structure, blockchain manages the trust among users sharing a common benefit as a variable in between. An updated ledger copy is a must for the transactions to be validated[7 8]. These transactions are then grouped to be published after a certain period. Publishing simply means appending the new blocks at the end of the previous block, and it is necessary to validate all previous blocks before publishing any new ones. Validating refers to checking the legitimacy of a block, and publishing a new block also states that the previous blocks are all verified. This creates a chain of blocks that can be traced back easily but are proved to be non-temperable. If tempered the transaction couldn't match with all the previous blocks and their nonce and hence the transaction gets canceled and would never make it through validation step[5 6]. On top of this, heavy cryptography can be added to make these blocks even more secure.

B. Software Defined Network

SDN was born at Stanford University in 2006 [1]. Although it is a recent technology, it gained the interest of many industries due to its flexibility and control over the network. As shown in Fig. 2, the basic architecture of SDN having three parts- Control Plane, Application Plane, and Forwarding Plane. SDN separates the control plane and forwarding plane so that both can work on a different physical medium. The forwarding plane is nothing but the interconnected switches which form a physical network, follow the control plane's routing decisions to forward the packages.

ISSN: 2233-7857 IJFGCN

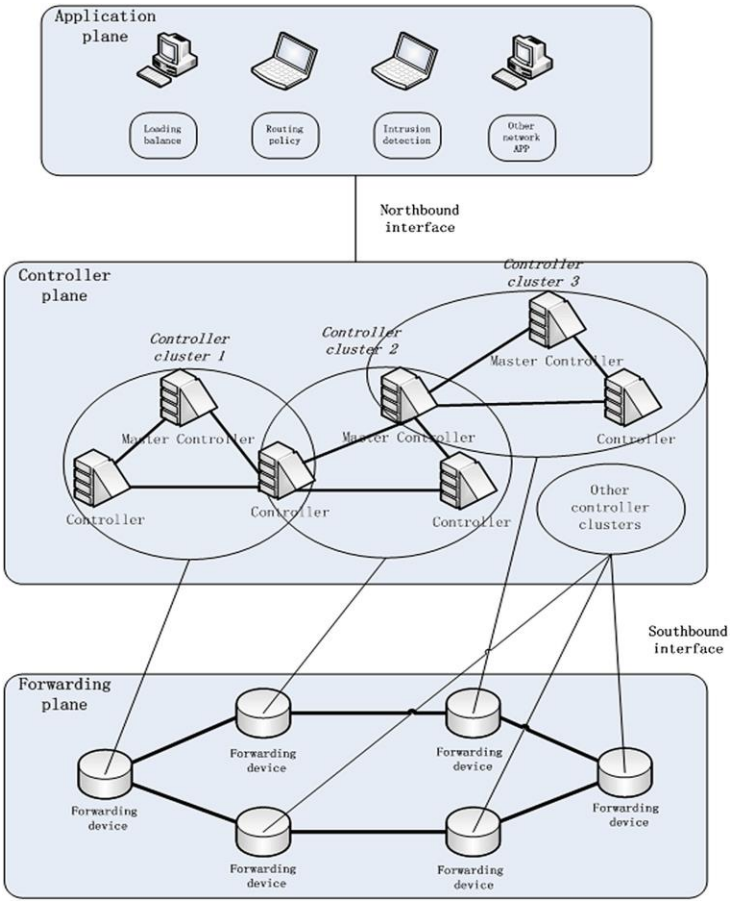

Fig. 2. Architecture of SDN

The control plane, acting as the brain of the whole network, collects the status of underlying running devices, formulating routing policies and providing instructions to the forwarding plane [1]. The control plane can be managed by a single central controller or in a mature SDN architecture it can be a group of controllers spread over various locations that assist the master controller which is responsible for the underlying plane's management.SDN meets the requirements of the developing technologies but there's always going to be a security concern. A few of the threats to the SDN are explained below.

Security Issues

Scalability and trust among users are some of the major concerns in SDN. Attacks like Denial of Service (DoS) and Distributed Denial of Service (DDoS) are one of the biggest security weaknesses in SDN. Switches have a limited storage capacity, and the flow table then cannot contain all forwarding policies. If the switch could not find a matching rule for the incoming packet, it sends a query, asking for suitable routing rule, to the controller and in the meantime stores the packet into its buffer. This caching technique makes the controller and switches vulnerable against the DoS attack, which floods the switch with large payload packages and the new incoming packages get dropped due to limited capacity of the switch meanwhile the resources of controller get exhausted handling the duplicate meaningless packages. DDoS attack, on the other hand, uses different sources unlike DoS, which uses just a single source, to flood the system, hence the name 'Distributed' DoS. DDoS attacks are performed on a much larger scale and are

ISSN: 2233-7857 IJFGCN

difficult to trace since it pings from various locations at the same time and hence is much more disastrous for the system[1].

III. DESIGN

In the proposed system we use the blockchain technology to build a security system for SDN. Blockchain has certain properties that make it secure against attacks like DoS and DDoS. In the proposed system, each node of the SDN is turned into a blockchain node and the distributed authentication system has been set up for every transaction or the resource request. By making every end-user system a blockchain node, each such system will contain an updated copy of ledger which will hold the detail of every block. The transaction here is referred to as a block, each request which a user sends to the controller for its services is considered a transaction hence a block. Each block is verified by the distributed authentication system and the decision then is recorded in the ledger.

Each system being a node will have a public and private key. The public key can be seen by every other node on the network, which will be matched to the private key which is a 32-bit alphanumeric code. Every user can refer to this public key of a certain user to communicate or to send requests. With these keys recorded in the ledger system, the controller will know the exact count of the active nodes easily. As the immutable property of blockchain, each system or node can request only once and cannot send the duplicate requests. These requests acting as a block will have a unique nonce and the blocks containing the same data or nonce will never make it through validation state and hence the attacks, such as DoS and DDoS, which uses duplicate requests from one system will never make it to the controller.

The end-users or the devices can be virtually made as blockchain nodes with the help of etherium, which is the platform for developing blockchain applications. It can be used to integrate the blockchain technology into SDN. The variable shared here is resources and services, which acts as virtual assets.

IV. CONCLUSION

This paper states the implementation of blockchain technology to solve the security and resource-related problems of SDN. With the help of blockchain's immutable property, the security for SDN is insured, and the authentication for the resources or services is distributed which forces the trust keeping resources as a variable. This distributed authentication makes the system more robust. Etherium is used to create a virtual system that makes every user a node of blockchain and every request from the user is considered a block with a unique nonce which then gets verified by the distributed authentication system, and on successful authentication, the ledger which every node holds is updated. Also, the new users which has to be attached to the SDN can be authenticated since every ledger holds the public key of every device in the network, hence connection from any new unauthenticated device is ignored and terminated.

ACKNOWLEDGMENT

This work was supported by the Computer Department of Sinhgad Technical Education Society's, NBN Sinhgad School of Engineering.

REFERENCES

[1] Zhen Yao, Zheng Yan. "Chapter 27 Security inSoftware-Defined-Networking: A Survey",Springer Science and Business Media LLC,2016.

ISSN: 2233-7857 IJFGCN

[2] H. Sukhwani, J. M. Martínez, X. Chang, K. S. Trivedi and A. Rindos,"Performance Modeling of PBFT Consensus Process forPermissioned Blockchain Network (Hyperledger Fabric)," 2017 IEEE36th Symposium on Reliable Distributed Systems (SRDS), HongKong, 2017, pp. 253-255.

[3] Dhumane, A., & Prasad, R. (2015). Routing challenges in internet of things. CSI Communications.

[4] [2] Dhumane, A. V., Prasad, R. S., & Prasad, J. R. (2017). An optimal routing algorithm for internet of things enabling technologies. *International Journal of Rough Sets and Data Analysis*, *4*(3), 1–16.

[5] Shwetambari Kharabe, C. Nalini," Robust ROI Localization Based Finger Vein Authentication Using Adaptive Thresholding Extraction with Deep Learning Technique", Journal of Advanced Research in Dynamical & Control Systems, Vol. 10, 07-Special Issue, 2018.

[6] Shwetambari Kharabe, C. Nalini," Using Adaptive Thresholding Extraction - Robust ROI Localization Based Finger Vein Authentication", Journal of Advanced Research in Dynamical & Control Systems, Vol. 10, 13-Special Issue, 2018.

[7] Shwetambari Kharabe, C. Nalini," Evaluation of Finger vein Identification Process", International Journal of Engineering and Advanced Technology (IJEAT), International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8 Issue-6S, August 2019.

[8] Udayan Birajdar, Sanket Gadhave, Shreyas Chikodikar, Shubham Dadhich, Shwetambari Chiwhane, "Detection and Classification of Diabetic Retinopathy Using AlexNet Architecture of Convolutional Neural Networks", Proceeding of International Conference on Computational Science and Application, online 05 January 2020, pp 245-253.

ISSN: 2233-7857 IJFGCN