Overview of SDN with Blockchain over Cloud Environment

Nidhi M. Sukhdeve
Department of Computer Science and Engineeriing,
G. H. Raisoni College of Engineering,
Nagpur, India.

Apeksha Sakhare
Department of Computer Science and Engineeriing,
G. H. Raisoni College of Engineering,
Nagpur, India.

Saurabh Gangwar
Scientist/Engineer (SE),
Regional Remote Sensing Centre
Central Nagpur ISRO, Nagpur, India.

Abstract:- **Software-defined networking (SDN) has advanced to interchange the ordinary style of the prevailing community. To enhance the security of the SDN community deployed in the cloud environment. This paintings proposes to enforce SDN enabled blockchain implemented over cloud. The SDN controller ryu might be used for community management and orchestration. This assessment paintings offers an summary of common safety issues with SDN as soon as joined to clouds, describes the appearance principals of the these days added Blockchain paradigm and advocates the reasons that render Blockchain as a enormous safety component for solutions wherein SDN and cloud are worried.**

Owing to which there is a substantial increase in the amount of users' data (personal, enterprise, financial, etc.) flowing over Internet, thereby, attracting serious threats from the malicious users. Various security solutions have been proposed and implemented to protect users' data from unknown threats. Majority of these solutions are realized employing traditional networking techniques that are complex and extremely difficult to manage. These techniques rely on manual configuration of devices resulting in policy conflicts, which may compromise the network security.

This issue may be addressed by using adopting Software Defined Networking (SDN) paradigm which presents a networkwide visibility, centralized control, bendy community structure and ease of control, by using separating manage plane (network controller) and the facts aircraft (forwarding gadgets). The controller monitors, manages and controls the behaviour of the forwarding gadgets the use of OpenFlow protocol. In this paper, we suggest and validate an SDN based totally community-extensive firewall with the aid of exploiting the abilties of OpenFlow, as one of the safety answers to restrict the suspicious traffic coming into in a community.

I. INTRODUCTION

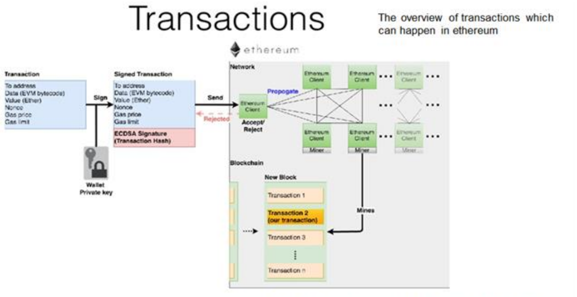
Software Defined Networking (SDN) is the framework for network architectures that separates manipulate common sense of community from data forwarding aircraft making the network management extra honest. The manage common sense of the community is carried out in a logically centralized community controller making switching and routing gadgets as simple statistics forwarding devices. Famous companies like Microsoft, Google, Yahoo, Facebook, and Verizon have invested within the development of open standards for SDN. OpenFlow protocol is the open standards that permits conversation between the control aircraft and the statistics plane in SDN environment. The controller makes use of OpenFlow protocol to skip switching, routing, load balancing or firewall regulations onto facts plane gadgets

. Firewall may be visualized as a protection device based on preset security policies used for tracking and controlling incoming and outgoing packet site visitors in a community. A conventional firewall acts as a barrier among an inner relied on network and an outdoor untrusted network together with the Internet. It is excessive quality to put into effect firewall with SDN community architecture because the centralized control in SDN encourages the enforcement of community-huge safety rules and prevents insurance collision.

In this paper, a firewall protection framework is proposed this is designed to provide community-significant protection at the same time as examining incoming flows into the network. This answer gives the community administrator complete control over protection policy implementation and change; concurrently making the firewall evidence against threats thru tracking network flows.

II. BLOCK CHAIN

A blockchain can be a suburbanized, distributed and public virtual ledger it really is wont to record transactions across numerous computer systems so any involved record cannot be altered retroactively, with out the alteration of all subsequent blocks. This permits the individuals to verify and audit transactions severally and relatively inexpensively. A blockchain data is managed autonomously employing a peer-to-peer network and a allotted timestamping server. They are echt by mass collaboration hopped-up by means of collective self-pastimes Such a fashion allows robust paintings go with the flow anywhere contributors' uncertainty concerning facts security is marginal. The use of a blockchain removes the characteristic of infinite reliability from a virtual plus. It confirms that each unit treasured became transferred one time, finding the lengthy-status drawback of double disbursement. A blockchain has been delineated as a price-change protocol. A blockchain will keep name rights because of, once properly created to element the alternate settlement, it provides a document that compels provide and attractiveness.



Source: https://www.slideshare.net/ConorSvensson/java-and-the-blockchain

Fig. 1. Transactions over blockchain

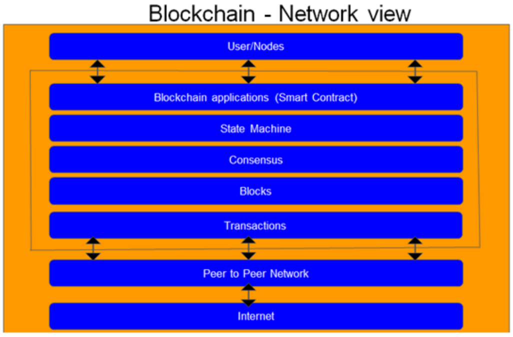


Fig. 2. Blockchain – Network view

A. Etherium Blockchain

1.Conceptualized by way of Vitalik Buterin in Nov 2013.
2.Turing Complete Language
3.Allows development of arbitrary programs (clever contracts)
4.First release "Frontier" and the cutting-edge launch "homestate release" and very last release as "serenity"
5.Serenity-Proof of Stake(Caster), Scalability, Privacy, EVM.
6.The vision of Web three.0 idea – People, programs, data, and web related collectively.
7.DNS, Search Engines and identification on the net – decentralized in internet three.0 and Etherium to realize this.
8.Native foreign money ether ETH- difficult forked model.

Blockchain consists of three constituent technology operating in mixture as: Cryptographic hashing, asymmetric public-key cryptography, distributed P2P Computing
i)Each block header consists of a root-hash of the entire chain, along side the hash of transactions in the block.
ii)This bits of records inside the block header are used to create an encryption seed ,which in flip generates a DAG document, which expands to 1GB and serves as akind of father-up element tray for the proof-of-paintings set of rules, which hashes together chunks of records from the DAG with a view to search for a winning nonce price with a purpose to validate the block.
iii)Etherium debts use a couple of cryptographic keys, one public and one private, to encrypt transactions sent to their respective digital machines, set of rules used is known as secp256k1 curve to carry out encryption.
iv)Etherium makes use of the elliptic-curve –based totally encryption protocol call as an ECDSA algoritm permits for a smaller key length, which reduces storage needs and transmission requiremants.
v)Etherium uses SHA-256

III. ADVANTAGE

A. Background

1. Most of the SDN improvement paintings on features, not safety, these SDN are at risk from new attack vectors which were actually not feasible earlier than with conventional networks.
2. In conventional networks, hosts/servers at the network would usually be at hazard from attack, however now with SDN, new APIs and therefore vulnerabilities exist for the network itself.
3. To reveal this trouble, once a single rogue detail together with a switch or compute element, injected with the aid of a hacker, is normal with the aid of a SDN, the hacker can be capable of view, reproduction, modify, disrupt communications on the community.
4. Therefore any safety answer need to be able to scale and feature the performance to allow dozens of valid factors in at once, even as rejecting a single rogue element from a hacker.

B. Solution

A solution in which some thing which takes place on the SDN is captured in a forensically auditable and unchangeable log – the blockchain. If hackers try and cowl their tracks by means of also hacking into the log server and changing the history of activities, because of the truth the blockchain and its records exist in lots of lots of places without delay so any alteration would be rejected by the blockchain peers.

IV. LITERATURE SURVEY

In latest beyond, many works are executed in SDN to discover its abilities for boosting cease-to-stop network safety. Several techniques are proposed to put in force numerous protection rules for deploying firewalling principles, as it's miles the first detail to shield malicious attacks at the community. SDN controllers like RYU, Floodlight, POX, and so forth. Have provided assist for firewall modules for trying out and development. The simple structure of firewall in SDN surroundings is proven in Fig. 3.

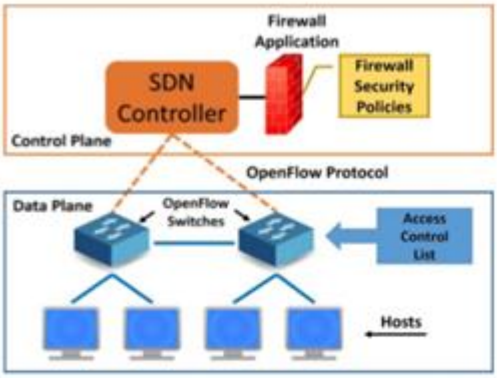


Fig. 3. The basic structure of firewall in SDN environment.

In a recent work, Nife et al. proposed a notion of reactive stateful firewall and methods to optimize its performance using S-Table and SecPolTable in addition to the flow table. However, there are still ambiguities regarding the implementation and validation of the proposed idea. In another study, Vasaka et al. devised a reactive stateful firewall (using raspberry pi) that increases throughput, by distributing network traffic through multiple links consisting firewalls (for inspecting suspicious traffic) and a redundant link (bypassing the non-suspicious traffic).

Zerkane et al introduced a new approach for proactive stateful firewall in SDN environment with an Orchestrator as a network security management utility running on the application plane. Orchestrator can communicate to multiple controllers and deploy securities policies in firewall application residing in controllers. Tran and Ahn presented FlowTracker stateful firewall with ability to learn network topology and deploy security policies in order to reduce redundant entries in flow table that filter network traffic.

V. PROPOSED FRAMEWORK

The SDN framework consist of network controllers strolling at manage aircraft, numerous records forwarding gadgets (e.g. Switches, routers, and so on.) at information aircraft and network programs jogging on top of controllers. The community applications teach controllers to put into effect community services which includes switching, routing, load balancing, firewall, etc. OpenFlow protocol exists among manage plane and facts aircraft to set up communication between controller and statistics plane gadgets. The first model (model 1.0) of the OpenFlow had simplest 12 in shape fields and single go with the flow desk. The proposed framework is based totally at the brand new version of the OpenFlow (model 1.5) which functions 44 healthy fields and a couple of float tables. Though open flow ver 1.5 turned into released around 2014 [9], studies on this topic is confined. The proposed framework is the implementation of firewall utility on an open-source SDN controller running on OpenFlow ver 1.5 specifications. In order to make sure scalability, four OpenFlow enabled switches connecting 4 distinct person systems are deployed. The Ryu framework is performing as an SDN controller because it supports OpenFlow model 1.5 specs. The firewall rules are set to both permit or block the packets based totally at the header records along with source and destination mac cope with, IPv4/IPv6 deal with, port numbers, and so forth. These firewall regulations are primarily based on the suit fields laid out in OpenFlow Switch Specification ver 1.Five because these specifications will govern destiny OpenFlow enabled devices. The firewall module collects records about the related and available switches inside the community and hence the community administrator can set regulations for every character switch inside the firewall utility. The firewall software constantly video display units get right of entry to manipulate listing set up on switches to make certain it isn't always changed by any external or inner gadget and upon detection, utility re-path the flows in network as safety measure.

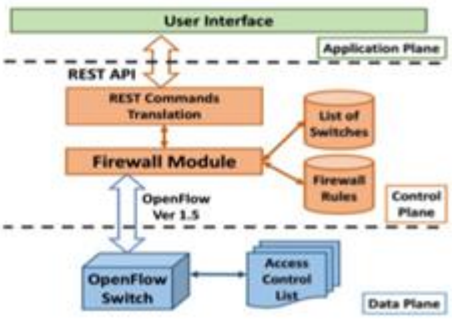


Fig. 4. The block diagram of SDN firewall applications

A. Building Blocks of Firewall Model

The fig. 2 represents building blocks of SDN firewall having firewall application running on control plane in SDN controller while it is being connected to OpenFlow switches. The firewall application consist of four major components – Firewall Module, REST commands translation, list of switches and firewall rules. The firewall module is the heart of the firewall application that will co-ordinate with the controller module for implementing firewall rules in the network devices. The network administrator can access, set, delete or modify firewall policies on user interface through REST Application Program Interface.

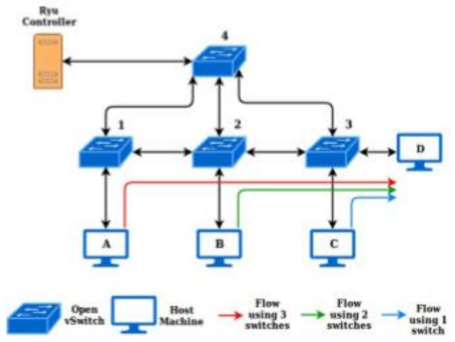


Fig. 3. (1) Traffic flow through 3 switches, (2) Traffic flow through 2 switches, (3) Traffic flow through 1 switch

Fig. 5. Openflow Switches

A list of firewall rules governs the security policies of the network and it consist of separate rules for individual switches or individual VLANs in a switch. At data plane, every switch consists of access control list and is loaded with number of firewall rules received from firewall application. These firewall rules are based on the match fields specified by OpenFlow Switch Specifications ver 1.5.

VI. CONCLUSION

SDN has revolutionized flexible network policing while providing programmability for better control over data plane configuration. Additionally, OpenFlow protocol has enabled precise packet filtering to incorporate MAC/IP/TCP layer features in simple data forwarding device. This helps in the implementation of network wide security policies without affecting the network performance in a large network. Tests carried out on the prototype network for three different packet types namely, ICMP, TCP and UDP; show that SDN based firewalls can be promising techniques for defending malicious threats in large networks. The proposed firewall is validated on GNS3 platform, and implementing such firewall with OpenFlow v1.5 has elevated the hopes to include future versions of OpenFlow protocol for better security prospects. Apart from implementing firewall security policies, the application can include security features like deep packet inspection, intrusion detection to enhance security of the network.

In this paper, we propose a centralized blockchain-based security framework over cloud environment in SDN-enabled etherium blockchain. Exploiting the immutable feature of blockchain, the accountability of the source message is validated. With the support of the blockchain-based framework,we present the trust management for the vehicular system in case that malicious nodes may claim fake messages or messages may be tempered. Both theoretical analysis and experiment results illustrate the efficiency of our framework since the detection accuracy of the malicious nodes are significantly improved.

REFERENCES

[1] Hyunmin Kim, Jaebeom Kim, Young-Bae Kao "Developing a Cost-Effective OpenFlow Test bed for Small-Scale Software Defined Networking". Ajou University, Korea

[2] K. Bhushan and B. B. Gupta, ``Distributed denial of service (DDoS) attack mitigation in software de_ned network (SDN)-based cloud computing environment," *J. Ambient Intell. Humanized Comput.*, vol. 10, no. 5,pp. 1985_1997, May 2019.

[3] Qinlong Huang, Yixian Yang and Yuxiang Shi, “SmartVeh: Secure and Ef_cient Message Access Control and Authentication for Vehicular Cloud Computing”. In: Sensors, Vol.18, Issue 2 (February 2018).

AUTHORS PROFILE

Nidhi M. Sukhdeve, Bachelors Degree In Computer Science And Engineering From Gurunanak Institute Of Engineering And Technology Nagpur, Mtech IInd year in Computer Science and Engineering from G. H. Raisoni College of Engineering Nagpur

Saurabh Gangwar, Scientist/Engineer at RRSC-C ISRO Nagpur, Bachelors degree in Electronics and Communicatio from Institute of Engineering and Technology Lucknow, Masters degree in Computer Science and Engineering from Indian Institute of Technology Hyderabad, Research in the field of Blockchain security, Satellite image processing and mobile applications

ApekshaV.Sakhare Assistant Professor ,GHRCE,Nagpur, BE in Computer Engineering ,Master Degree in Embedded System and Computing (CSE), Teaching Exp: 9 Years. Research in Deep Learning, HCI.