International Journal of Advanced Trends in Computer Applications
www.ijatca.com

Security Techniques in Software Defined Network

[1]Shalini Kumari, [2]Saumya Gupta, [3]Dr. Sandeep Singh Kang
[1,2,3] *Computer Science and Engineering, Chandigarh University, Mohali*
[1]shalinidas281@gmail.com, [2]gupta98sept@gmail.com, [3]sandeepkang.cse@cumail.in

Abstract: *Another technique for building and tracking networks has been created by software-defined networking (SDN), but it has also updated the assault surface formed by the organization.SDN offers numerous designs that permit straightforward moderation of particular sorts of assaults, for example, DoS, and permit further work to alleviate certain assaults. In any case, SDN regularly presents new imperfections that are absent in customary organizations, for example, a nonappearance of correspondence between the control plane and the information plane. A few new advancements and strategies have been recommended to conquer shortcomings in SDN security and some extra work may likewise be applied to fix them. Current SDN work explores many measurable patterns that contribute to the state of SDN technology implementation. Because Open Flow is SDN's most common implementation is currently being used in production environments, and IOT of research has been done to use and develop the protocol. There is anyway another exploration pattern that has work that is for the most part pertinent to SDN, including designs that give more adaptability than Open Flow. The expected study will probably follow these patterns by enhancing Open Flow protocol and suggesting more general alternatives, and this research will include further development of network design testing tools and research into Open Flow enhancements when used in production environments. This work presents a study survey review of current SDN security research and other work done in the field of SDNs that is relevant to security and a forecast of future SDN security research directions.*

Keywords: Software design networking, SDN security, Security evaluation, control plane, open-flow.

I. INTRODUCTION

Software-Defined Network (SDN) is a principle of system management that supports detaching the information plane of the organization from the control plane of the organization. The data plan contains the entirety of the information communicated through the organization, for example, bundles, and the hardware utilized for sending it, for example, switches. The control plane contains all rationale and devices liable for choosing whether and where to send information in the data plan. Such two planes are combined on the same computers by conventional networks, requiring each device to make its own forwarding decisions based on distributed routing protocols. Then again, SDN empowers the control to intend to have a worldwide perspective on the organization, allowing policies to be enforced that take into consideration the whole network state and not what's exposed to one device [1].

Software-defined network (SDN) is the dynamic organization innovation for handling conventional organization issues. It gives an incorporated perspective on the whole organization, by decoupling an organization's control plans and data plans.

The control plan is answerable during strategy AS organizations are filling in size and multifaceted nature, raising more prominent administration and calculated difficulties. Current organizations are progressively exceptionally heterogeneous with various gadgets, going from little sensors and machines to arrange gadgets like switches to a wide range of customers and workers and peripherals [2], planning and execution, and the data plans are in control for packet forwarding. Such frameworks additionally utilize various organization foundations, for example, wired, remote, and portable organizations. In quite a complex heterogeneous climate, network framework the executives, (for example, switches, and routers), client and gadget portability, dynamic organization fluctuation (because of gadget disappointment and organization associations).

Significant problems face themselves due to the drastic rise in security threats. A promising approach to tackling some of these issues is given by Software Defined Networks (SDN). The networking environment has been revolutionized by the Software-Defined Network (SDN). It produces become the panacea for customary systems administration issues

including merchant reliance, high depreciation costs, less programmability at switches, no headways, and so on SDN has presented adaptability by decoupling the whole organization engineering into three separate zones–Application, Control, and Infrastructure layer [3].

OpenFlow SDN has provided many networking benefits. It encourages straightforward, multivendor markets and a steady method to impart stream data between network gadgets. Open Flow supports the virtualization of the network and thus allows network convergence of computation and storage. Due to the standardization of OpenFlow, all organization tasks can be produced from a solitary perspective for example Regulator to SDN. Interest for OpenFlow-based SDN is that on account of the numerous advantages it offers of various brilliant gadgets [4].

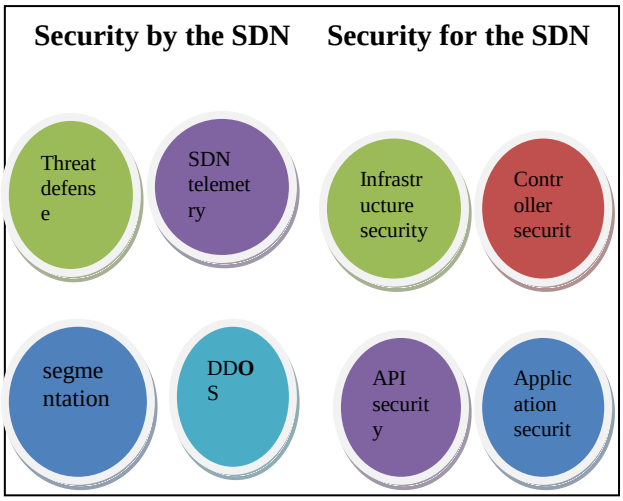

Figure 1: Shows what security should be provided by the SDN or what security we can provide to SDN

II. SDN ARCHITECTURES

Firstly, is the management plane, which is an assortment of organization applications that direct a product characterized by the organization's control rationale. Rather than utilizing an order line interface, SDN-empowered organizations use programmability to give adaptability and simplicity in executing new applications and administrations, for example, directing, load adjusting, strategy implementation, or a client support system.

Secondly, the savviest and basic layer of SDN engineering is the control plane. It contains at least one regulator that forwards the various sorts of rules and approaches utilizing the southbound interface to the infrastructure layer.

Thirdly, the data plan, also known as the networking layer, reflects the organization's sending gadgets (switches, routers, load balancers, and so on). It utilizes the southward APIs to speak with the control plane by acquiring the transmission rules and arrangements for applying them to the separate gadgets.

Fourth, a series of ASCII text file application programming interfaces (APIs) area unit the north-bound interfaces that permit correspondence in the center of the management layer and also the management layer.

Fifth, the east-west interfaces that are not yet normalized permit the numerous regulators to impart. They use notice and informing plan, or a unified directing convention, for example, BGP and OSPF.

Sixth, the southward interfaces permit the control plan to speak with the information plane, which can be immediately indicated as conventions that permit the regulator to move the sending plan's approaches. The OpenFlow convention for SDN-empowered organizations is the most ordinarily grasped and executed southward API [5].

III. LITERATURE REVIEW

In 2017 [2] Liu et al. presented the Middlebox placement concept. SDN transition middlebox and flow table power limitations are the main problems when middlebox and SDN mix together. The purpose of this study was to use SDN-based IoT middlebox to control data flow and enhance network stability and security. To this end, M-G, middlebox-based information move insurance. Model-dependent on SDN was proposed in IoT. M-G means to improve the accessibility of solidness. SDN-based IoT applications and to react effectively to organize dangers. They initially handled positions in the middlebox. Fitting positions are chosen to utilize a calculation for the arrangement choice which diminishes network inactivity. They also found the strength of the network. To adjust the heap around middleboxes and switches, an ILP pruning calculation and an LP detailing are conveyed there. Finally, they studied the handling of data flows. Safe mechanisms can protect against many attacks. The condition of a parcel is seen by utilizing the proposed dataflow the board convention, and the way is appropriately determined. Exploratory outcomes show that the proposed MG model and the relating conventions adequately handle data flow in middleboxes and enhance the security of the IoT network and stability.

In 2018 [1] Mukhonav et al. formulated the security problem and represented the aspects of object and environment concerning defense. This helped them to prepare descriptions of different risks, theories and policies, unified by shared security objectives, both for the object (the controller) and its operating environment, and to begin to shape practical safety requirements. Differentiating the rates which decide the composition of the functional safety requirements involves several security groups. In the initial

development of the controller's protection profile, a safety class with a minimum composition of practical safety criteria (fifth class) can be considered, and modified for a particular usage class. Under these conditions, MTUCI designed the design of the controller security profile of fifth security class Type "A" software-configured networks.

In 2018 [3] Byun et al., propose the IP producing danger of SDN-based security administration. SDN-based insurance administration blocks unconfirmed IP addresses across the whole organization, which can prompt the deficiency of the network of properties. The evasion technique utilizes the OpenFlow convention to decide the hindering reach for this assault. This tool is used by the SDN- based protection service to block malignant IP addresses inside the change port from which the bundle begins, and with financially savvy and simple methods we can forestall the deficiency of openness of information.

In 2018 [4] Varadharajan et al., presented a concentrated SDN strategy-based security design, permitting to make sure about between area interchanges and multi-space streams between various end hosts. This paper made important contributions to the ability to smartly distributed security services are service layer and hybrid security policy framework to secure multiple devices from attack.

In 2019 [5] Zheng et al. presented a model that applies IoT SDN technology, isolating intelligent control and information transmission in the passage layer, pre-situating the IoT security system sending, and making the security rules more flexible and efficient. The Hurst values can be determined in the specific security techniques to efficiently identify network traffic irregularities and network attacks according to network traffic's self-similarity.

In 2019 [6] describes the Security Evaluation Methodology has been identified allowing network security experts to identify accessible SDNs regarding insurance. The conversation and discoveries introduced in the paper will permit associations to carry out formal SDN safety evaluations and rely on the findings; decide which infrastructure to follow on the SDN. Established projected metrics can serve as guidance for patching security vulnerabilities found in the specified SDN infrastructure.

IV. OPEN FLOW AND TLS SUPPORT

SSL(Secure Socket Layer) is the mainstream technolo gy maintaining a stable network by preventing data fro m unauthorized users and helping to protect data integ rity[3].

TLS (Transport Layer Security) is a much secure updated SSL version that ensures that encryption algorithms are certified with the DSA, ECC, or RSA options. The Open Network Foundation correspondence determination OpenFlow doesn't make the execution of TLS in the organization mandatory yet characterizes it as discretionary as it were. There is no doubt that the standard appropriation of OpenFlow makes the organization adaptable yet conveys with it some security perils [4].

Figure (2) illustrate the steps involved by the SSL/TLS protocol that deals with SDN security:

- Step 1. To initiate the session, the “hello” communication is sent from the TLS/SSL client to the SSL/TLS server.
- Step 2. Server to Client follows an acknowledgment “hello”.
- Step 3. The server certificate and cryptographic check parameters are verified by SSL/TLS client.
- Step 4. Secret key information exchanged by the Client.
- Step 5. The client also sends certification parameters.
- Step 6. The server verifies client certification.
- Step 7&8. The connection of client and server is established.
- Step 9. The exchanges of data in the middle of Client and Server

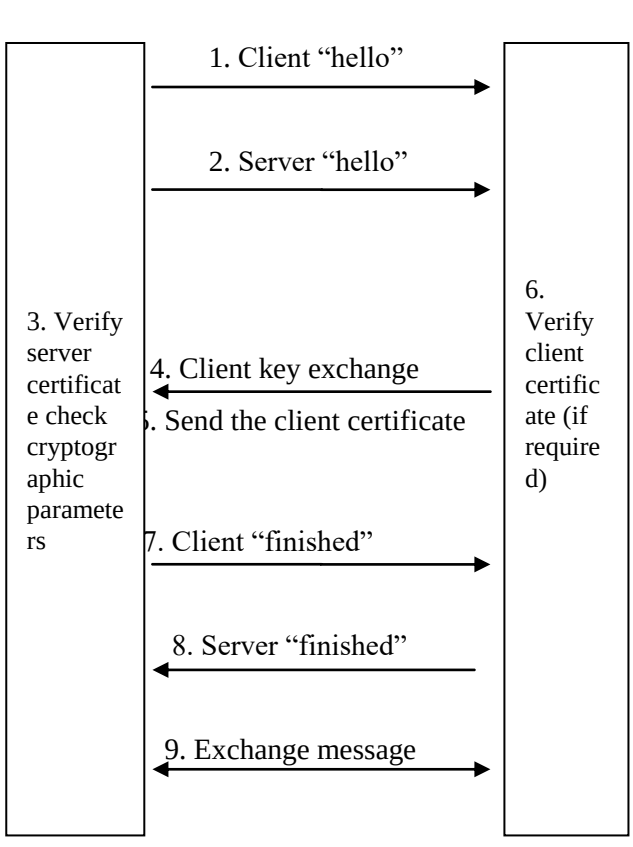

Figure 2: Client/Server Handshaking in SDN

V. OPEN FLOW SECURITY

Many of the latest SDN security research works use ordeal with the OpenFlow protocol. Three research categories apply to security for OpenFlow [5].

First, this is the work that aims to address the problems of scalability and fault tolerance that occur in the design of OpenFlow controllers. These problems are not specifically inspired by security apprehensions but are directly relevant because, as can be seen during a DoS attack, they progress the reliability of the network under load.

Second, the category is an investigation that addresses the security susceptibilities that are present in the description of OpenFlow. The head of these issues is the correspondence bottleneck between the data and the control plans that can be effortlessly settled by control traffic in specific cases.

Third, the group is to work using OpenFlow to overcome existing susceptibilities in the defense. Because of the network accessibility which is confirmed to the controller, applications may use the protocol to build network-wide policies that are more powerful than the conventional networks [7].

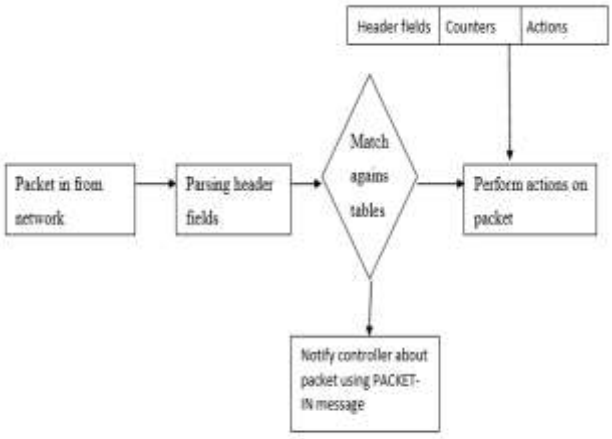

Figure 3: In switch basic packet forwarding with OpenFlow

A considerable lot of the weaknesses that should be tended to are created by the key advantages offered by SDNs, for example, detachment of the information plan and control plan.

Little work has been led to address these weaknesses and analysts are proposing some likely ways to deal with these weaknesses. The researchers defined numerous vulnerabilities as:

- Falsified traffic streams generated by broken or copied gadgets in the organization can be used either on the control plane or on the information plane to deny assets from various gadgets.
- Switch weaknesses: Attempts to abuse change weaknesses to bargain such gadgets. These assaults can prompt the abuse of other organization shortcomings [5].
- Communications control plane: Any attack between the data plane and the control plan that could deal with the protection of the correspondence channel can frustrate or even interrupt network exercises. Numerous assaults will endeavor to over-burden the channel of correspondence to keep the organization from working.
- Vulnerabilities of regulators: Similar to weaknesses of switch assaults yet unquestionably more genuine. At the point when a regulator is undermined, an aggressor probably has total organizational power.
- Trust among regulators and applications: most regulators don't set down trust rules for applications and there are no instruments for building trust. It is critical to believe applications working on regulators because a regulator application has a similar perspective on the organization as the regulator [6].
- Administration station weaknesses: similarly as the regulator should be made sure about from network assaults, so should the regulator programming gadgets. On the off chance that this gadget has undermined a regulator might be re-modified by an assailant, as opposed to attempting to impair it.
- Lack of dependable legal assets: OpenFlow doesn't give the way to comprehend large numbers of the issues that could happen in the organization and does exclude any confirmation instruments to check the wellspring of the insights given by the determination.

These issues exist in different routes in SDN and OpenFlow.

Security Flow Rules

A. North-bound Communication

The SDN controller receives configuration directions and safety flow rules from applications on the northward API [6].

- IA-3 (Identification and authentication of devices): every program should be genuine unambiguously before submitting any directions to the SDN controller.
- IA-7 (Authentication of the cryptographical module): All interactions should be attested to victimization the Federal informatics commonplace (FIPS) approved message authentication code rule via the north genus Apis and also the SDN controller.
- IA10 (Adaptive authentication): to stop quite one program from activity a similar perform, AN application manager has to be introduced as a security-enforced kernel.

- SC8 Confidentiality and integrity transmission: Correspondence between the Application Plan and the Control Plan must be encrypted in the SDN layer to ensure that data shared between the two layers is confidential [7].
- The option in contrast to the past arrangement is centered around Out-of-band SC-37 channels: make a committed organization through an out-of-band channel for all northward traffic.
- AU-2 Audit cases, AU-10 Non- repudiation: every solicitation or rule communicated between the applying and therefore the SDN regulator ought to be preserved during a log with fitting knowledge to follow the sender and therefore the receiver [8]. this may assist with testing responsibility if there ought to be a happening of arranging blunders or assaults from the applying plane.

B. Control Plan

- The Control plan is an SDN controller that receives rules from the Application plane for network installation, configuration, and management. The Data plane also receives information from the SDN controller about new devices and traffic[9].
- CP-7 Alternate process website and SC-36 Distributed process and storage: A load reconciliation power cluster of SDN controllers is needed.
- SA2 Resource allocation: The SDN regulator should be mounted on a devoted PC with sufficient figuring assets to deal with all traffic.
- SC5 Denial of service protection: Software for flow control must be implemented to detect potential DoS and DDoS attacks.
- SC36 Distributed Storage and Processing: the device running the SDN regulator should have in any event two organization interfaces with connecting total.
- SI4 Network Monitoring: A Host Intrusion Detection Network (HIDS) must be introduced on the SDN controller hosting computer to detect and track any changes in network configuration and to avoid anomalous activity[11].

C. South-bound Communication

All communication between the data plane and the SDN controller is included in this layer, so the NIST 800-53 ID and Authorization Scheme defines basic controls for this level of the SDN infrastructure.

- IA3 System identification and authentication: for all communication between the SDN controller and the Data plan, a bidirectional cryptographic authentication mechanism such as TLS must be used. This will stop any rogue system from being introduced in the Data Plane[12].
- Management of IA4 Identifiers: Identity managers can be used to classify each device on theData Plane.
- IA7 Authentication of the cryptographic module: The FIPS-approved communication authentication code algorithm must authenticate all communication between the data plane and the SDN controller[13].

D. Data plane

- IA7 Authentication of the cryptographic module: Authentication of each device is required on the Data Plan before any contact.
- SC5 Server security denial: To restrict traffic to the SDN controller, all switches must be programmed. To a degree, in the latest SDN implementations, the suggested checks from the above four classes are implemented. To demonstrate the applicability of the planned approach in the running SDN context, four well-known open-source SDN controllers, Open DayLight, ONOS, Floodlight, and Ryu SDN controls, were used to test the planned set of controls [14].

APPLICATIONS OF SECURITY IN OPENFLOW

Past exploration talked about as far as OpenFlow security has zeroed in on giving answers for known weaknesses in the convention or utilizing convention specific systems to ensure the organization's foundation. Nonetheless, a slight effort has been introduced on the usage of known organization danger moderation techniques, for example, interruption identification and firewalls, which shield end-have frameworks from assault. The recently introduced study has defined the target because of the organization, and also the OpenFlow convention specifically. Be that because it might, the work introduced by FRESCO and Mehdi et. al. speaks to different endeavors to execute recognize security applications within OpenFlow.

VI. DETECTION OF REVISITING ANOMALYUSING SOFTWARE DEFINED NETWORK

Mehdi, et. al. gift Associate in Nursing investigation of the effectiveness of 4 discovery calculations that exist for customary networks[15]. The scientists note that these calculations, at some level, work on the number of bundles that went through the organization per flow. By victimization normal OpenFlow network activity, the regulator is educated relating to the first bundle for every flow. By catching this first parcel notification, the calculation will understand the connection, and later on, insights may be a force from changes to choose the number of connected bundles.

By dominant what kind of square measure composed, different calculations may be upheld that require to own coarseness, for instance, crude range of protocol associations versus associations per-protocol port range, so on By victimization these OpenFlow highlights, calculations that pompously need every bundle will rather simply be incontestable with the first parcel, and allow any remaining bundles to be ready at line rates.

This application is a perfect representation of the utilization of OpenFlow capacities to actualize an organization's security arrangement. The specialists likewise current the OpenFlow usage as a more efficient execution than the conventional organization usage, as the calculations actualized don't have to see each parcel, yet just the quantity of bundles prepared.

VII. MEASUREMENT OF TOPOLOGY IN SDN

Network topology is an imagined portrayal of the overall condition of the organization; it interprets the actual connection among all organization hubs, which is a basic and center assignment in each organization [16, 18]. Estimating and refreshing geography assumes an urgent job in giving fundamental organization capacities, for example, directing, QoS, network the board, and glitch location and investigating. For instance, to make sure about an organization and lead a few safety measures for network assaults, the organization's geography is quite possibly the main one because of its huge part in the organization of the board [21]. Following parcel direction through the organization is one of the helpful and advantageous ways for confirming bundle sending in the information plane and ensuring network security, which implies precise and continuous geography estimation is basic [22]. Subsequently, to understand the previously mentioned capacities are concentrated regulators, it needs to have forward-thinking data about the condition of the organization continuously, which is geography disclosure.

Topology revelation may be important facilitate at the management set up and it'll support the licitly incorporated management and also the executives in SDN. during this section, we'll zero in on intradomain and interdomain earth science revealing methods applied in SDN organizations.

DiscoveryOfIntradomain Topology Based on OpenFlow

OpenFlow Discovery Protocol (OFDP) is a solid and generally utilized geography disclosure technique in SDN. It uses the LLDP convention to find linkage jump by the bounce. The entire strategy can be improved as all switch hubs will build up TLS with the regulator by handshake meeting in any case. During the meeting, control and switch trade crucial data and preinstall stream decides so the LLDP bundle will at last re-visitation of the regulator to complete geography data recovering [22]. At long last, the regulator will assemble the geography structure of the entire organization. Point-by-point data is a segment of three perspectives.

(1) First Stage. The regulator gets pivotal data about each hub in the organization. Switches set up TLS meetings with a regulator with its IP address and TCP port numbers. The regulator will recover the dynamic port number and comparing the MAC address of switches and relegate an extraordinary ID for each switch. The guide of ID and its comparing port data will be slowed down in neighborhood recollections.

(2) Second Discovery Stage. The regulator sent an LLDP parcel to each dynamic switch port which contains significant data like switch ID, port number, etc. When shown up, the switch moves the bundle to its neighbor hub. Due to the preinstalled stream runs, all LLDP parcels will be moved to the regulator through the Packet_In message. In this manner, the regulator settle got bundles, recovering switch ID and port number, and refreshing the planning table to get done with fundamental organization structure disclosure. The entire strategy has appeared in Figure 4.

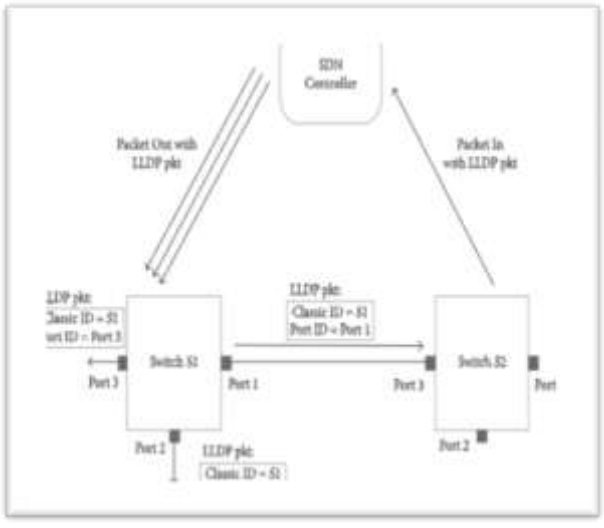

Figure 4: OFTD topology discovery procedure

(3) Third Updating Stage. At the point when the organization state changes (e.g., interface interference, port state change), this will trigger a synchronization in a geography update. The regulator will direct the previously mentioned measure again to acquire the most recent organization state.

OFDP [21] is all around planned and simple to actualize, yet the time cost, calculation asset utilization, and presented control overhead are generally high. Thus, in OFDP [20], these issues have been improved by lessening regulator sending parcel numbers which are restricting sent LLDP bundle number for each change to one. At the point when switches got the LLDP bundle, these parcels will be copied and altered, adding the comparing MAC address of the moving port number. These copied bundles at that point are moved to all access ports in a switch.

The exploratory outcome demonstrates that, in the wake of applying OFDP, 45% control overhead and 40% CPU assets have been saved contrasted and the first form. Yet, over the long haul, the impediment of OFDP exists. When refreshing the entire organization structure, it is unavoidable to burn through countless figuring assets, cost an excess of time, and press regulators' presentation with a weighty weight. Organization QoS can barely be ensured from one viewpoint and versatility and execution of SDN networks are influenced on the other [22]. This requires another geography disclosure convention.

VIII. CONCLUSION

In this work, we've got mentioned the definition of SDN and also the role of the various OpenFlow protocol specifications, that area unit a way of implementing SDN-based networks, was explained. We have shown varied SDN applications that in varied fields boost network management and operation, business networks and middlebox routing, security problems, and interdomain routing. Thought of the protection flow rules is an important contribution of this paper. In this, we tend to mentioned north communication, south communication, and also the management plane.

REFERENCES

[1]. Liu, Y., Kuang, Y., Xiao, Y., & Xu, G. (2017). SDN-based data transfer security for Internet of Things. IEEE Internet of Things Journal, 5(1), 257-268.

[2]. Mukhanov, A., Petukhov, A., &Pilugin, P. (2018, October). "Common Criteria" and Software-Defined Network (SDN) Security. In 2018 International Scientific and Technical Conference Modern Computer Network Technologies (MoNeTeC) (pp. 1-6). IEEE.

[3]. Byun, M., Lee, Y., & Choi, J. Y. (2019, February). Risk and avoidance strategy for blocking mechanism of SDN-based security service. In 2019 21st International Conference on Advanced Communication Technology (ICACT) (pp. 187-190). IEEE.

[4]. Varadharajan, V., Karmakar, K., Tupakula, U., & Hitchens, M. (2018). A policy-based security architecture for software-defined networks. IEEE Transactions on Information Forensics and Security, 14(4), 897-912.

[5]. Zheng, S. (2019, May). Research on SDN-based IoT Security Architecture Model. In 2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC) (pp. 575-579). IEEE.

[6]. Midha, S., &Triptahi, K. (2019, January). Extended TLS security and Defensive Algorithm in OpenFlow SDN. In 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 141-146). IEEE.

[7]. Abdou, A., Van Oorschot, P. C., & Wan, T. (2018). Comparative analysis of control plane security of SDN and conventional networks. IEEE Communications Surveys & Tutorials, 20(4), 3542-3559.

[8]. Fawcett, L., Scott-Hayward, S., Broadbent, M., Wright, A., & Race, N. (2018). Tennison: a distributed SDN framework for scalable network security. IEEE Journal on Selected Areas in Communications, 36(12), 2805-2818.

[9]. Al-Alaj, A., Krishnan, R., & Sandhu, R. (2019, October). SDN-RBAC: An Access Control Model for SDN Controller Applications. In 2019 4th International Conference on Computing, Communications, and Security (ICCCS) (pp. 1-8). IEEE.

[10]. Nikoue, J. C., Butakov, S., & Malik, Y. (2019, January). Security Evaluation Methodology for Software Defined Network Solutions. In 2019 International Conference on Platform Technology and Service (PlatCon) (pp. 1-6). IEEE.

[11]. Duan, Q., Ansari, N., & Toy, M. (2016). Software-defined network virtualization: An architectural framework for integrating SDN and NFV for service provisioning in future networks. IEEE Network, 30(5), 10-16.

[12]. Braun, W., &Menth, M. (2014). Software-defined networking using OpenFlow: Protocols, applications, and architectural design choices. Future Internet, 6(2), 302-336.

[13]. Smyth, D., McSweeney, S., O'Shea, D., &Cionca, V. (2017, July). Detecting link fabrication attacks in software-defined networks. In 2017 26th International Conference on Computer Communication and Networks (ICCCN) (pp. 1-8). IEEE.

[14]. Ramaswamy, V. (2017, July). Quantifying the Scalability of Software Defined Networks with Dynamic Topology. In 2017 26th International Conference on Computer Communication and Networks (ICCCN) (pp. 1-7). IEEE.

[15]. S. A. Mehdi, J. Khalid, and S. A. Khayam. Revisiting Traffic Anomaly Detection using Software Defined Networking. Recent Advances in Intrusion Detection (RAID), pages 1–20, 2011

[16]. Bakshi, K. (2013, March). Considerations for software-defined networking (SDN): Approaches and use cases. In 2013 IEEE Aerospace Conference (pp. 1-9). IEEE.

[17]. Alhanani, R. A., &Abouchabaka, J. (2014, November). An overview of different techniques and algorithms for network topology discovery. In 2014 Second World Conference on Complex Systems (WCCS) (pp. 530-535). IEEE.

[18]. Liu, F., & Li, T. (2018). A clustering-anonymity privacy-preserving method for wearable IoT devices. Security and Communication Networks, 2018.

[19]. Tarnaras, G., Haleplidis, E., &Denazis, S. (2015, April). SDN and ForCES based optimal network topology discovery. In Proceedings of the 2015 1st IEEE Conference on Network Softwarization (NetSoft) (pp. 1-6). IEEE.

[20]. Pakzad, F., Portmann, M., Tan, W. L., &Indulska, J. (2014, December). Efficient topology discovery in software-defined networks. In 2014 8th International Conference on Signal Processing and Communication Systems (ICSPCS) (pp. 1-8). IEEE.

[21]. Khan, S., Gani, A., Wahab, A. W. A., Guizani, M., & Khan, M. K. (2016). Topology discovery in software-defined networks: Threats, taxonomy, and state-of-the-art. IEEE Communications Surveys & Tutorials, 19(1), 303-324.

[22]. Zhang, H., Cai, Z., Liu, Q., Xiao, Q., Li, Y., &Cheang, C. F. (2018). A survey on security-aware measurement in SDN. Security and Communication Networks, 2018.