An Approach for Supervising the Security Threats using Software Defined Networks

Harshitha M R,Harshitha J S,Brunda K S, Shrihari M R

Abstract: Providing protection for the network is major significant subject by continued existence of systems which are allied by means of network in this world, which broadcast information regarding every part of circumstances in our life and occupation. The systems which have fine security to a network would support business in addition to, it decreases the hazard of diminishing fatality in favor of data theft and sabotage. The framework of software defined networking (SDN) disjoins the data and control planes. The fundamental set of connections (network) structural design is inattentive from applications, the state of a network along with brilliance are logically integrated. It increases security for a network with the help of overall visualness of the network condition wherever a collision could be straightforwardly decided commencing the understandably united control plane.TheSDN has some types of mechanics together with network virtualization, functional separation along with computerization by practicability by programs. Based on the packets flow through the network the control plane generates outcomes, while the plane of data shifts packets from one position to another position. Even so, open protection difficulties, like man-in-the middle attacks, denial of service (DoS) attacks, along with saturation attacks. The design of SDN authorizes networks toward actively observes the transfer passage and analysis the risk to simplifies network disputation, safety procedure modification, and safety examine inclusion. In this paper, we examine safety threats to appliance, the planes of SDN that is data and control plane. The safekeeping designs that protect all the planes are defined and succeeded by different safety ways for network-wide security in SDN. Highlighting the present and upcoming safety difficulties in SDN and expecting guidelines for safe SDN in this paper.

***Index Terms*: SDN, OpenFlow, network security, SDN security, application plane, control plane, data plane.**

I. INTRODUCTION

The network administrationis reduced by softwaredefined and SDN is enabling invention in communicating networks. And it developed as one of the main important network infrastructures.This skill uses cloud computing , that promotes network administration and allows programatically well-organized network arrangement. Sequentially that it advances the network supervising and presentation. The fixed structural design of conventional networks is circulated and composite but the existing networks need more suppleness and simpledamage assessment. The SDN disassociates the progressing method of network packets (data plane) out of the routing method (control plane) and experiments to integrate network cleverness in a single network constituent with disconnecting aprogressing method of network packets (data plane) out of the routing process (control plane). One or more monitors of the control plane are measured at the same time as the intellect of network of SDN and alsothe complete cleverness is incorporated. Nevertheless, when it comes to safety, scalability and supplenessdefects are owned by the cleverness unification and it is considered as the major subject of the SDN.It going to disjoint the control plane of networkcommencing from thedata planeand also calling as forwarding plane. In order to actstraightforward on decisions from the control plane [1] the progressing plane that is data planeis surrendered and the control plane is sensibly integrated.The latest control functions in SDN could be executed through composing logic-basedsoftware in the control plane that set up the conclusion reason in the data plane with the help of typical interfaces. And the control plane has (NOS) network operating system thatoutlines the whole set of connections to variousbenefits and utilizationswhich are executedabove of the control plane.

In the structural design of SDN, OpenFlow is mainly recognized and extensively executed. And here theguidelines of networkand methods are executed as OpenFlow applications that are work together by means of the control plane from side to side the north-bound API (application programming interface) of the control plane. The functionaries of control plane are executed in an OpenFlow organizer that cooperates by means of the forwarding plane in the course of the OpenFlowset of rules (south-bound API). The applications of OpenFlow-based SDN are establishedwhich make use the fundamental network framework and organize a variety of objectives at execution time. Consequently, the network traffic control is transmitted beginning the infrastructure to the supervisor. As an outcome, the operators of network would achieve morealtitude of network control, mechanization in addition to hike through the assist applicationsof SDN. The SDN increases safeties of a network through the integrated organize of network activities, worldwide visualness of the network situation and

Revised Manuscript Received on May 20, 2019.

Harshitha M R, Department of Computer Science, S.J.C Institute of Technology, Chickballapur, India.

Harshitha J S, Department of Computer Science, S.J.C Institute of Technology, Chickballapur, India.

Brunda K S, Department of Computer Science, S.J.C Institute of Technology, Chickballapur, India.

Shrihari M R, Department of Computer Science, S.J.C Institute of Technology, Chickballapur, India.

execution-time exploitation of interchange progressing set of laws.

The nationalized environment of networking in SDN approvesaccomplishing network broad safetymethods and tempers the hazards of strategy clashes. The applicationsconcerned with network security(e.g., security monitoring application) could appeal stream fragments from end to end the manager starting the information path. Subsequent to safety examination, the safety claim could readdress the information lane essentials to obstruct the interchange, redirect to the middle boxes of security or limit the interchange surrounded by a network authority. Furthermore, revising safety rules in SDN wishesrevising the safetymechanisms or accumulating security divisions to the manager stage, other than varying the hardware or revising its firmware.

Conversely, predictable networks include huge firms of seller-definite physically conformable strategy extend transversely networks. And these strategies are hardwired by means of particular innovations used to direction, manage and examine information stream established taking place purpose definite sense in every one machine. Therefore, it would be hard to faultlessly merge them into a one field beside by means of every the occupancyset of rules, appliances, along withcombinations. The effect would be that legacy network infrastructurebe deficient in worldwide perspective of the network situation and alsohazards in expandingalong with preserving logical set of connections-large procedures. The indicated difficulties along with weaknesses in combination build it inferior for preserving steady and strong network safety. On behalf of example, altering or revising safety procedures in this kind of systems in the get up of diversities in interchange or incursionsis basically impossible along with its also expensive.The security for a network in legacy network infrastructures is well thought-out as an add-on thatentrust on physically conquerable boundary-positionedresults. In order to execute a high-level network safetyrule, the network managers have to organize everymachine by means of retailer-exact low-level guidelines.

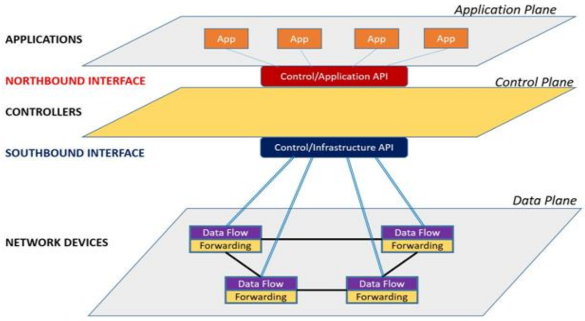

Fig 1: Software defined networking- high level architecture

Nevertheless, physical compositions of network safetymechanics as firewalls, incursion recognition/avoidance structures (IDS/IPS) and IPSecmechanics on extensive firmof machines are horizontal to arrangement failures,outer and inner field procedure disputes which effect in severe safetycracks and coercion. A significant learning on firewall arrangement failures [4] displays that company firewalls impose policy sets which break famous safety rules and outcome in safetycracks owing to labor-intensive low-stage structures in each and every of the machines.

As a result of sensibly coordinating the control plane of network and introducing programmability, SDN allows safety mechanization and execution-time consumption of safety policies and rules. The Network safetymachines liverying from SDN could reply to network exceptions and fake interchange settings at runtime. To detailed the operations of the SDN infrastructure, the main three well-designed layers or SDN planes are offered in Figure 1 itembodies :

- Application Plane: It comprises SDN appliances in favor of a variety of functionalities, like as network administration, procedure execution, along with safety methods.
- Control Plane: It is a reasonably coordinated organize framework whichbounds the NOS, preserves worldwide observation of the network, and implements hardware entrancements to SDN appliances.
- Data Plane: This is the grouping of progressing essentials used to advance interchangestreams derived from commands from the control layer.

The Network safetyfashions could be executed the same as applications in the SDN application plane. And those applications will obtain the network condition or supply data starting the control plane of network throughout the north-bound interface (App-Ctrl-API). In the same way, security applications can gather samples of packets through the control plane. After security examination, safety appliances/machines could transmit the interchangeconceding to superior stage safetyrules by the control plane using the southbound API (Ctrl-Infra-API). Dissimilar conventional networks, information behavior policies in SDN are executed as software sections somewhat than enclosing them in the hardware, consequently, grantingexecution-time implementation of safetyrules and policies. Nevertheless, SDN comprising it does possess difficulties and restrictions in conditions of safety, flexibility, and stability. Safety would be taking place the front position of these difficulties. Because a centralized manager is answerable for running the whole network, safety negotiation of the manager could cause to be the entire network conceded. In addition, safety faults in manger data path message could direct to dishonest right to use and convention of network resources. On one hand, SDN enables applications to interrelate with the control plane to access network sources, organize fresh methods and influence the manners of the network. Then, protecting the network from malevolent appliances or unusual activities of appliances is a severe safetydifficulty in SDN. The network security is critical in order to achieve the networking knowledge and conversation networks have to offer back-to-back communication safety.

The examination of network safety in SDN is offered in [5]. Scott *et al.* [5] contributes in a detail summary of security difficulties in SDN. Illustrate some of the obtainable frameworks for intensify safety measures in SDN. Even thoughsdn has providing safety measures as an benefit, at a standstill there are fewer SDN defense keys.

Though, [5] is restricted in extent and do not wrap the latest approaches in SDN safety. We endeavor by providing a wide-ranging and up-to date general idea of safety measures in SDN by declaring security difficulties and keys associated to individual SDN planes i.e., the application plane, control plane, and data plane. We also illustrate network-wide security keys and safety measureadvancement platforms in SDN, classify safety evaluation according to the ITU-T safety propositions, and I detail represent costs of diverse safety measureplans. Segment II explains safety in past programmed for network designs are showed in the topics of SDN in segment III.

II. SAFETY IN COMPUTEINTERCONNECTIONS: THE PAST

The safety has been overwhelming duty in the message networks owed to the fundamental set of connections difficulties, tenancy and edge-dependent safety keys that are complicated to handle, and the weedy design of uniqueness in IP networks. Similarly, the construction of the network that describes events for practice of the essential communications [6], derives the troubles arise from the framework, is refined with safekeeping provocations and is inactive to modernization. Consequently, numerous ideas have been locate ahead for (re)architecting the Internet to restrict its innate restrictions, and to reduce its difficulties and safety amenabilities. In this section, we talk about those ideas which either had an brunt on fabric safekeeping or fabric safekeeping has been its significant aim above and beyond other targets.

A. Active Interconnections

The concept of Active interconnectionswas projected to permit nodes scheduling using user inserted software's [7]. In these active fabric, nodule carry out modified calculation on the weight that passageway through them. As a result, the nodules can be customized to perform according to client or appliance prerequisites. There are some of the advantages of active interconnections. They are
i) distribution of universalset of rules, ii) latent to execute well-grained appliance-meticulous ultrapractical in chosen nodules inside the fabric, and iii) client determined customization of the framework to allowquickdistribution of pioneering utilities [8].

The key dispute for vigorous fabric was to protect vigorous nodules from unpleasant user-insertedsoftware's. Like an effect, vigorous protection [9] and supplementary protection techniques [10] were anticipated to make certain that a node's safety and protection through verification and permission approaches. Nevertheless, difficulty in supervision and safety measures of active nodules lasted exigent responsibilities in active fabrics.

B. 4-Dimension Technique

In this approach, Greenberg *et al.* [11] correlate the brittle scenery of communication fabric to the multifaceted environment of manage and administration planes in conventional interconnections. The need of synchronization between map-reading and protection approaches effect in a flimsy set of connections and safety blunders is exemplified here. Hereafter, a spotless-schedule technique is projected known as the "*4-Dimensiontechnique*," named subsequent to the four planes of choice, spreading, detection, and facts. This 4-Dimension construction entirely re-factors the functionalities of a system and split the fabric power from the redirecting substrate. It is recommend by authors that a network design ought to be based on three key main beliefs i.e., i) system-level targets, ii) system-wide perspectives, and iii) straight organize [11].
Fabric security goalsare measured as system-level aims and fabric safety measures is measured as an essential fraction of the fabric supervision in this 4-Dimension design. In order to allow innovative, easier, additional tough, added consistent, and supplementary sheltered power and executive set of rules as of a incorporated verdict plane, division logic was planned. The resemblance in theory aims 4-Dimension and Software defined networks shows that the its design is the modern edition of the 4-Dimension design. Likewise, OpenFlow has rebound from the thoughts of the 4-Dimension mission as affirmed in [12].

C. SANE

The Secure Architecture for the Networked Enterprise (SANE) [13] is a spotless-schedule safety design for activity interconnections. The intend aims of this construction consists of plans that helps easy but influential likely procedures, self-determination from topology and fabric apparatus, association coating safety measures, fortification of topology and benefitsdata from illegal contact, and integrated description and carrying out every the schemes [13]. Domain Controller (DC),which is a part of SANE architecture thatdoes threemajor tasks. Firstly, the users, hosts, and switches are authenticated by DC, and a balanced key with everyone in support of protected communication is maintained. Secondly, DC advertises and controls right to use to existing services. Thirdly, every part of the connectivity in a SANE network is managed by DC.

In order to resolve the complication of safety frame of reference used in business, a plan of SANE appeared. Conventionally, arrangement of theboxes is multifaceted, frequently needy on system topology and situated on location or substantial piers that formulate fabric supervision tricky and effect in breakable fabric safety. Effortless high-endschemes which are uttered in the centerwere enabled by SANE and are compulsory by a solitary well-grained technique within the system. Thisdifficult provocations were resolved with the lend a hand of centralized verdict building and dropping the amount of loyal and constructed apparatus with uncomplicated and plainly-reliableredirectingentities. This construction has been unmitigated to Ethane [14]that is planted on the theory of additionalset up in activity interconnections [15].

D. Ethane

Even though, the chief thesis of the Ethane scheme [14] was to integrate the manage judgment of a fabric, it splits the architecture from the framework in a manner that the forwarding switches are performing on command of the integrated organizer.

The planning of Ethaneincludesof aintegrated regulator with worldwide vision of the set of connections, easy and dumb Ethane switches with a easy surge chart and a protected conduit to the organizer. In addition to this, appropriate strategy supervision in the system, protection has been well thought-out as an essential fraction of the system supervision and for this reason uniqueness-based contact power has been measured for the construction. It follows the effort of the SANE [13] design and has a likeness to SANE. On the other hand, unlike SANE, the security of Ethaneis measured as a separation of system supervision, and appropriate to reverse-congruity of Ethane, it can be set upquickly.

This Ethane is constructed just about three central ideology. Firstly, policies that govern the network are stated over high-point labels. Secondly, schemesgoing to find out paths that the packets go behind. Hence, this makes it simple to manage travel and set up innovative safekeeping benefits. For instance, a strategy may need to facilitate definite travel ought to be forwarded to incursion finding systems, safety center boxes, and firewalls etc. The last fascinating theory is the sturdy obligatory between packets and their starting point. The locationswhich are used these days are self-motivated and revolutionize habitually. Therefore, it is awfully intricate to unfailingly narrate traffic to their starting place. Schemes affirmed over high-point labels in ethane and sheltered obligatory amid packet headers and the bodily entities that sent them make possible tracking users and machinery still if they move. Accordingly, it is a well-built and divergent safekeeping characteristic of Ethane that ought to be incorporated in Software Defined Networksframework. Ethane is well thought-out to be the forerunner of the contemporary OpenFlow departure of Software Defined Networks which can be seen in the architectural semblance of together techniques.

III. SOFTWARE DEFINED NETWORKING

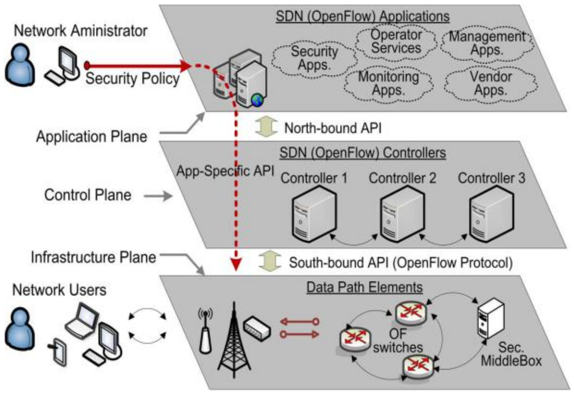

Fig 2: SDN reference structural design with system components.

APPROACHES AND OPERATION

The system organize along with redirecting functions is divided by SDN. Individual redirectingappliances divides the power judgment and implemented in a sensibly incorporated regulator. Therefore, the controller that manages the information plane turn into theintent of uncomplicated redirectingappliances.

To make the network power to be programmable, statistics planes and control planes has to be separated and the fundamental frameworkhas to be preoccupied for the functions as well as fabricaccounts. Specifically, Software Defined Networks design dis-accumulates habitual perpendicularly incorporatedfabric loads on the way to get better fabric aspect rate or else to adapt system process for dedicated platforms. This regulator is departing to be discussing and approaching commands in factual-instant downward to the system objects in SDN design. Appliances can be built on peak of the program stratum to consume, having the program stratum beyond scheming the housewares underside and control heterogeneous network assets [16]. The system designers and directors have to answer hurriedly to the varying industry necessities which was the most important aim of the SDN design. With no to handle the substantial switches,system designers be able to outline travel since the middle regulator by means of the program to set up, transmit or obstruct travel either internationally or in unstable degrees downward to specific sachet surfaces[17].This Software Defined Networks orientation structural design as well as the relations flanked by the Software Defined Networks stratumis offered in Figure. 2. System supervisor know how to put safety schemes for the fabric all the way through the function layer and transmit system traffic to unusual safety structure or central-boxes by means of the power layers as shown in Figure. 2. Furthermore,through the assist of the Software Defined Networks regulator, the unpolished of the sanctuary measures can be continued to singledischarges.

While OpenFlow [2] is well thought-out to be the de-facto customary of Software Defined Networks, the majority of the sanctuary structures as well as ideasare based on OpenFlow. Consequentlywe portray the three layers of Software Defined Networks in agreement by way of the OpenFlow design underneath.

A. OpenFlow: Enabler of SDN

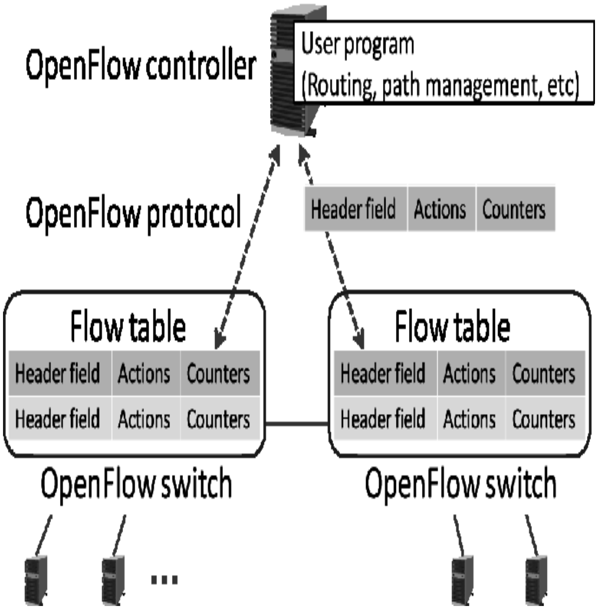

Fig 3: OpenFlow structural design

SDN’s three tiermethod has been implements using theOpenFlow; a novel method for connecting net with purveyor-atheist border, e.g., the OpenFlow protocol sandwiched among the control and data planes.SDN has a leading technology, which has explained logically centralized program organizer by OpenFlow[2]. This OpenFlow’s network redirecting appliance should talk. Hence, SDN technology is made possible to put into practice and set upin current networks. A clear unified examination of the set of connections is provided by the OpenFlow controller; thus making it simpler, and also simple to spot network frailness, incursions, and implementing safety measureschemes [18]. On top of the control planes, safety applications can be implemented to organize network protection services.

B. Application Plane

SDN authorizes appliance toward connection and handle the performance of set of connection components with the use of control layer. Advantages of applications are the visibility of set of connections properties in the organizer , can appeal the network status, and ease of access of network properties in particular ways. There is a need to couple applications in between physical or virtual properties e.g., in support of physiography and connection finding, protecting functions, domain name maintenance, internet address conversion benefits and deploying virtual secretive connection. So, internet users and examine managers need to control, operate and set policies by using applications for different set of connection manager, compositions and management benefits [19]. The control phase implements an conceptual sight and source data of the full set of connections essentials to SDN appliances. In OpenFlow, the manager conceptual the set of connections difficulty, assembles set of connections information from beginning to end southbound API and maintains a consistent map of the complete set of connections. Information of the set of connections provided to appliances through the utilize of north-bound API of a manager. Initially, OpenFlow is a normal option to build up set of connection operations in the type of OpenFlow appliances. So, safety actions are developed on top of the OpenFlow manager with a dissimilar type of set of connections as safety appliances which are explained in the following fields. .

C. Control Plane

In SDN, The particular set of connections nodes are implemented in a separate reasonably centralized plane in the control plane is taken away. The SDN manager [20] is referred by the entity that develops in the control phase functionalities. The SDN manager is able for organization and managing the whole set of connections by the NOS through a middle vantage point with a worldwide view of all the network properties. The NOS collects set of connections information using APIs to check and control a net abstractly much like an operating system. A consistent and central programmatic crossing point to the whole set of connections which is provided by the operating system for connection, such that methods developed on top of the operating system carry out the specific association tasks. The manager is applicable for flow settings in data-path elements (e.g., OpenFlow switches) is being an integral part of SDN, such that the entire flow processing in the data-path is based on commands as of the controller. In the OpenFlow SDN architecture, the protocol provides an open and advance approach for the manager to interact with switches [2]. When a packet of a new flow arrives in the switch, the switch checks its flow table for flow rules equivalent to that specific packet. If a matching entry for the flow exists, commands for that particular flow are executed; otherwise the flows are transferred to the manager. The manager then sets the flow rules in the switch flow tables to either transfer the flow packets to a specific port or drop packets entering from that specific source. The initial design of OpenFlow considered a single OpenFlow manager for ease. Recent OpenFlow architectures support multiple managers which can be circulated in the network to complete higher scalability and accessibility.

D. DataPlane

The SDNs’ separation of control and data planes refers to creating the forwarding devices ease and distantly hand able via open interfaces. Forwarding devices such as switches, virtual switches, routers and access points can be configured and planned for separate functions together with traffic isolation and virtualization via a control process call from the controller with a secure communication channel. The most suitable example of SDN forwarding devices is the OpenFlow switch. OpenFlow switches are easy and, therefore, future-proof as advancing policies are imposed by the manager software to a certain extent by the switch hardware or firmware. Any Ethernet switch or router containing flow tables can be planned to be an OpenFlow switch with the OpenFlow protocol. When planned to an OpenFlow switch, the flow tables of a switch or router be use to keep flow entry through an connected set of actions for every flow [2]. A OpenFlow switch may have an expandable position of functionalities other than the least necessities be so as to should have; i) a table which flows through procedures connected by each flow for handing out the flows ii) a protected channel to the manager to agree to interactions of commands and packets; and iii) The OpenFlow procedure given that an open and advance methods for the manager to contact through the switch. An OpenFlow switch must be responsible of advancing a packets allowing to the outflow rules installed in the flow tables. OpenFlow switches or common function Ethernet switches or routers enabled with OpenFlow. Layer 2 and Layer 3,does not support normal processing, while a later have OpenFlow protocol and alliance additional as advanced applications [2].

E. Standardization Activities and Industry Experience

SDN have collected exciting consideration as of the management and academia. This necessitate quick consistency foremost toward beginning actions in Standard Development Organizations (SDOs), management and society alliance. The *de facto*principles which frequently move toward in the appearance of open resource implementations that are considered as standardization bodies transport results.

The Open Networking Foundation (ONF) has been recognized because a manager for SDN principles which improves a acceptance of SDN with a advancement of the OpenFlow protocol when an open advance in support of manager information path communication. ONF has planned in several technological working groups (WGs) for structural design and construction, extensibility, arrangement and organization, promoting applications, experimenting and interoperability. The SDN Research Group (SDNRG) as to targeted on investigation condition intended for the development of the Internet created by the Internet Engineering Task Force (IETF). IETF has available in the Internet Drafts on safety requirements in SDN, safety of OpenFlow switch, SDN and NFV safety construction. The International Telecommunication Union's Telecommunication sector (ITU-T) has started Study Groups (SGs) to develop recommendations for SDN, and a Joint Coordination Activity on SDN (JCA-SDN) to manage the Organization task. The information that represented SDN safety allowing to the ITU-T safety recommendations.

SDN as a new revolution in the technologies of the network which has applicable for this type of industry. In March 2011 Deutsche Telekom, Google, Microsoft, Yahoo!And so on formed the Open Networking Foundation (ONF) to support SDN technologies [18]. Adopting the SDN technology, surpass $35 Billion by 2018. Individual may reduce as ofthe aim of the future of networking lies in SDN.

IV. CONCLUSION

This SDN design increases network safety through worldwide perceptionof the network status. The general distribution layer collects required data about security necessities of diverse resources , services, hosts, and distributes safety initiating instructions to network fundamentals to implement safety rules in SDN. The set of connections control phase and enforcing connection programmability are focusing, it may caneffect the robust and scalable safety fulfillment, one hand, that establishes original safety difficulties, on the other hand. In this paper, offered safety weaknesses and strengths of SDN. While doing we have focused security amenability in application, control and data phases of SDN, and after that represented safety explanations for these planes. We also summate safety approaches that can intensify the set of connections safety in SDNs. Afterward offered safety keys allowing to the safety references of International Telecommunication Union-Telecommunication(ITU-T) and in a few words we defined the expenses related to security keys. To our perception, the mainly insecure element in the SDN design is the centralized controller. As a outcome, controller weakness has previously been described and researched from different views as well as controllers protection from appliances, expandable controller and ease of use, flexibility and assignment, and safety from DoS and DDoS attacks. The OpenFlow switch laws as safety which has achieved additional concentration of the examine society, while they characterize the definite interaction. Though safety operations are initialized and achieved, the safety of the operational plane itself is a safety test. Furthermore, interaction safety among managers and switches in OpenFlow is susceptible because of a possible utilize the TLS and DTLS. A greatly achievable that new safety risks may appear along the ongoing deployment of SDN mechanisms. Likewise, the risk space will most probably increase, because safety risks presented in conventional set of connections willbcirculate through SDN-particular safety difficulties. Though, SDN desired by bringing improvement in interaction networks and therefore, automatic safety methods will be implemented to facilitate quick variance recognition and fast reply for security. Already obtained literature on set of connections safety SDN certifies a reality to SDN determinesfast set up of cost-effective security services.

REFERENCES

1. B. Raghavanet al., "Software-defined internet architecture: decoupling architecture from infrastructure," in Proc. 11th ACM Workshop Hot Topics Netw., 2012, pp. 43–48.
2. N. McKeownet al., "OpenFlow: Enabling innovation in campus networks," ACM SIGCOMM Comput. Commun. Rev., vol. 38, no. 2,, Apr. 2008.
3. H. Hamed and E. Al-Shaer, "Taxonomy of conflicts in network security policies," IEEE Commun. Mag., vol. 44, no. 3, pp. 134–141, Mar. 2006.
4. A. Wool, "A quantitative study of firewall configuration errors," Computer, vol. 37, no. 6, pp. 62–67, Jun. 2004.
5. S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "SDN security: A survey," in Proc. IEEE SDN4FNS, 2013, pp. 1–7.
6. D. Clark, R. Braden, K. Sollins, J. Wroclawski, and D. Katabi, "New Arch: Future generation Internet architecture," Def. Tech. Inf. Center (DTIC),FortVelvoir, VA, USA, Tech. Rep. AFRL-IF-RS-TR-2004-235, 2004.
7. D. L. Tennenhouse, J. M. Smith, W. D. Sincoskie, D. J. Wetherall, and G. J. Minden, "A survey of active network research," IEEE Commun.Mag., vol. 35, no. 1, pp. 80–86, Jan. 1997.
8. D. L. Tennenhouse and D. J. Wetherall, "Towards an active network architecture," in Proc. DARPA Active NEtw. Conf. Expo., 2002, pp. 2–15.
9. Z. Liu, R. Campbell, and M. Mickunas, "Active security support for active networks," IEEE Trans. Syst., Man, Cybern., Part C, Appl. Rev.,vol. 33, no. 4, pp. 432–445, Nov. 2003.
10. S. Murphy, E. Lewis, R. Puga, R. Watson, and R. Yee, "Strong security for active networks," in Proc. IEEE Open Archit. Netw. Programm.,2001, pp. 63–70.
11. A. Greenberg et al., "A clean slate 4D approach to network control and management," ACM SIGCOMM Comput. Commun. Rev., vol. 35, no. 5, pp. 41–54, Oct. 2005.
12. Z. Cai, A. L. Cox, and T. E. N.Maestro, "Maestro: A system for scalable OpenFlow control," RiceUniv.,Houston, TX,USA, Tech.Rep. TR10-08, 2010.
13. M. Casadoet al., "SANE: A protection architecture for enterprise networks," in Proc. Usenix Security, 2006, pp. 137–151.
14. M. Casadoet al., "Ethane: Taking control of the enterprise," ACM SIGCOMM Comput. Commun. Rev., vol. 37, no. 4, pp. 1–12, Oct. 2007.
15. Y. Jarraya, T. Madi, and M. Debbabi, "A survey and a layered taxonomy of software-defined networking," IEEE Commun. Surveys Tuts., vol. 16, no. 4, pp. 1955–1980, 4th Quart. 2014.
16. S. Namal, I. Ahmad, S. Saud, M. Jokinen, and A. Gurtov, "Implementation of OpenFlow based cognitive radio network architecture: SDN&R," in Wireless Networks. New York, NY, USA: Springer, 2015, pp. 1–15.
17. M. Liyanage, A. Gurtov, and M. Ylianttila, Software Defined Mobile Networks (SDMN): Beyond LTE Network Architecture. Hoboken, NJ,USA: Wiley, 2015.
18. S. J. Vaughan-Nichols, "OpenFlow: The next generation of the network?" Computer, vol. 44, no. 8, pp. 13–15, Aug. 2011.
19. T. Nadeau, "Software driven networks problem statement," Network Working Group Internet-Draft, Sep. 30, 2011. [Online]. Available:https://tools.ietf.org/html/draft-nadeau-sdn-problem-statement-00

20. H. Xie, T. Tsou, D. Lopez, H. Yin, and V. Gurbani, "Use cases for ALTO with software defined networks," Working Draft, IETF Secretariat, Internet-Draft, 2012.[Online]. Available: https://tools.ietf.org/ html/draft-xie-alto-sdn-use-cases-01

AUTHORS PROFILE

Harshitha M Ris pursuing the Bachelar of Engineeringdegree with the Department of Computer Science ,S.J.C Institute of Technology, India.

Harshitha J Sis pursuing the Bachelar of Engineeringdegree with the Department of Computer Science ,S.J.C Institute of Technology, India.

Brunda K Sis pursuing the Bachelar of Engineeringdegree with the Department of Computer Science ,S.J.C Institute of Technology, India.

Shrihari M R, assistant professor, computer science department, SJC Institute of Technology. His research interest includes System software related work, SDN based security awareness.