A Study of SDN Architecture and Security Threats In Software Defined Networking (SDN)

Shad Hassan[1], Safdar Tanveer[2], S.S.Khalid[3]
[1]Dept of Computer Engineering
[2, 3]Assistant professor, Dept of Computer Engineering
[1, 2, 3] Jamia Hamdard University, New Delhi , India

Abstract- *Software defined networking (SDN) is a new technology that is designed in order to make the network more fast and flexible. We all know that today's networks are static, slow and in addition to this they are also allocated to single services as well. With the help of this new emerging technology one can create a network that handles the different services dynamically. With the help of Software defined networking(SDN),network administrators may automatically and also dynamically manage and control the large number of network devices, services, traffic paths, topology etc. Basically SDN is not a mechanism but simply an architecture by which networks are controlled by software applications as well as by a centralized controller called SDN controller. The main focus of this paper will be on the security threats and how these threats can be eliminated are surveyed. It reveals the important features of Software Defined Networking(SDN) and also discuss the Architecture of SDN and the security threats in detail.*

Keywords- Software Defined Networking(SDN), Architecture, VAVI, SAVI, Open Flow.

I. INTRODUCTION

We all know that due to the continuous development and in-depth application of cloud computing and also due to the Internet of Things(IOT) [5],[6], the architecture in case of traditional networks was not fulfilling all the requirements of current industries some of the examples of this are 5G Wireless networks [7], Internet of vehicles [8] etc. In order to fulfil the requirements of current industry fields researchers proposed a new model that was an innovative one but still needs a lot of modification in terms of various parameters. The new proposed model was Software Defined Networking(SDN).This new emerging technology will increase flexibility and also innovation of IOT as well in the industries [9],[10],[11]. Software defined networking is a new architecture that simply separates the network control plane from data forwarding plane [1]. In simple words we say that SDN decouples the control plane from hardware and is implemented in software. The important question which needs to be answered is why we move towards SDN? In traditional networks the network controller we were having was very much slow to manage and it was based on old commands as well as controls. So in order to attain speed and automation which was not possible in traditional networking then the new emerging technology came into existence that is SDN. In SDN the two important parameter's i.e., Speed and Automation are the key requirements of SDN. In traditional networks a lot of administrative work was required which makes the system more complex. As far as SDN is concerned, less administrative work is required which makes the system easily operable and also reduces complexity. So the main thing in SDN is such networks are fast, flexible and also there is less complexity. Basically SDN is an open technology and effective as well as compared to traditional ones which we were having in the field of networking. Some of the most important advantages of SDN includes: Flexibility, More Interoperability, Greater Innovation, and Cost effective solution etc. The most important advantage is cost effective solution when we have SDN based interfaces. The two important parameter's required in SDN plays an important role as we are going to make association with Cloud & Multitenant networks, for these speed and automation is key [4]. Before SDN we were having many issues some of the important ones were complexity, manual configurations, inconsistent policies, inability to scale etc. In present time every organization is having growing demands like additional hardware requirements as well as software changes. These requirements may become expensive so it is important to take SDN technology into account so that we can meet the growing demands of the user. Apart from this discussion about SDN it also helps us in server virtualization in order to increase resource efficiency which means we can use the resources in an optimal way and also reduce complexity, in addition to this management becomes fast as well.

In order to understand what actually the concept of "SDN" is, then we need to know how the packets of data are managed?. Every time a packet of data reaches to the destination i.e., at a switch or router, it is the firmware which tells the hardware where to forward the packet and send all the packets to the destination through the equivalent path but the advanced smart switches' equipped with ASICS can recognize different types of packets and treat them differently based on the fact that ASICS are programmed [13]. The main disadvantage of such solutions is, they are very much expensive that is the reason SDN is good because it separates the control from the networking hardware's firmware and control is being assigned to the network administrator. The job of the network administrator is to shape the network traffic from a central console without changing the settings of individual switches. Which means Administrators can change network rules and even block certain packets with great console [13]. Hence we conclude that SDN is very important for the future of networking as we all know that how much fast the concept of cloud computing is increasing so cloud computing having a Multi-tenant environment(multiple users can share single application and database) allows more well-organized and flexible control of traffic loads.

This paper is organised as : Section I provides the basic knowledge about the SDN, Section II provides us the brief idea about the architecture of SDN and its layers, Section III explains some basic features of SDN, Section IV deals with the security issues that may arise in SDN and also the possible measures with which we can eliminate them, Section V&VI contains Conclusion followed by the References.

II. ARCHITECTURE OF SDN

According to [1] a basic SDN architecture is presented in fig(A) and fig(B). Generally the architecture of SDN is divided into three important layers i.e., Infrastructure Layer, Control Layer and Application Layer respectively and is shown in fig(A).The APIs between these layers comes under north bound APIs and south bound APIs .The application interfaces between the control layer and infrastructure layer comes under southbound interface and the APIs between control layer and application layer comes under the northbound interface. The centralized controller called SDN controller in the SDN architecture allows us to impose consistent policies easily. We can also configure the common networking functionalities with the help of supported APIs. Basically the deployment of different services in SDN, such as security, access control, bandwidth management, Routing, traffic engineering, quality of service, energy optimization can be configured much easily. According to [1] the basic objective of the SDN developers is to ensure multi-vendor support.

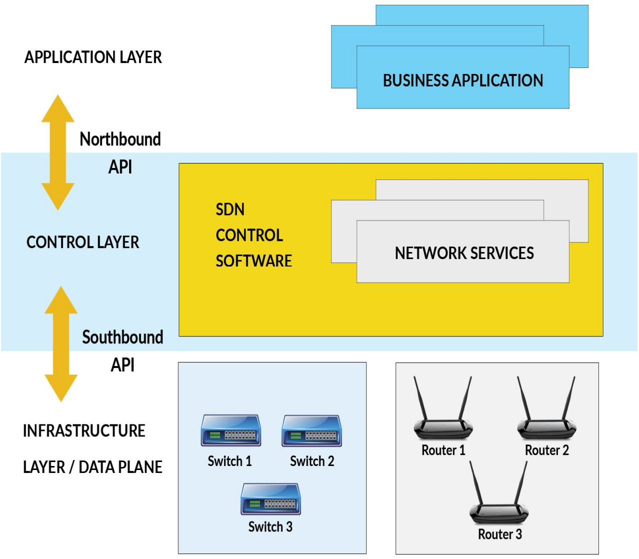

Fig.(1)Software-Defined Network Architecture, [1]

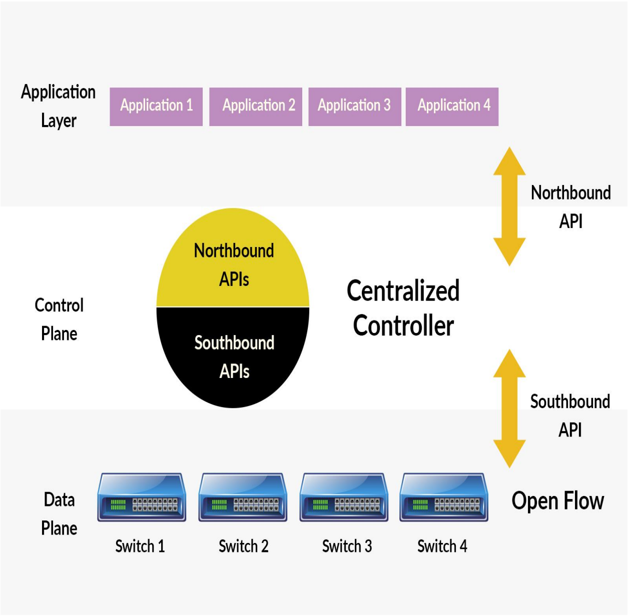

Fig (2). Simple Architecture of SDN.

a). *INFRASTRUCTURE LAYER:*-This is the bottom layer of the SDN architecture also known as Data plane, where different forwarding equipment lies. This layer of SDN is responsible for moving packets and frames across the network. This layer receives information from Control layer and based on this information, move packets across the whole network. It consists of both physical devices and virtual network devices like routers switches, firewalls etc. Basically the forwarding equipment rely on the control layer. In simple words we say that infrastructure layer deals with the delivery of packets and also processing based on the state in network devices(routers, switches etc) and end points e.g. TCP, IP, Ethernet etc

b). *CONTROL LAYER*:- This is the middle layer in SDN architecture commonly known as the brain of SDN which simply establishes the state in routers, switches etc and determines how and where the packets are forwarded. This is the plane where decisions are made regarding the forwarding of packets and frames. This is the layer of SDN architecture which is responsible for the management and control of the entire network i.e., run applications in order to control network flows. The control layer simply take the service requests from the management plane i.e. the application layer and maps all the service requests into the infrastructure layer in the most favourable manner. Usually this layer of SDN receives its configuration from the application layer. In case of distributed environments, it should be noted that control layer contains multiple SDN Controllers which work in synchronization manner. The Agents in control plane connect the SDN control logic to Application plane [3].

c). *APPLICATION LAYER*:- In technical perspective we can say this layer of SDN simply means the tools like APIs, SSH, SNMP etc. Basically the application layer of SDN architecture is the kernel part of control layer [1] and is also known as Management Plane. This is the layer where Management applications, Business applications, Cloud Applications place their demands for the network until the control layer. It consists of network services, applications and automation tools that are used to interact with control layer. Basically It provides an open interface in order to communicate with other layers in the SDN architecture.

III. IMPORTANT FEATURES OF SDN

In this section, we will focus on the features of Software defined networking (SDN) in detail. The features of SDN will tell us How actually we can attain the enhancement and efficiency of networking, in addition to this also how this thing will make it a promising technology in the future in the field of networking and big data analytics as well. The features of SDN may also have a great impact on the security of SDN as well. Some of the important features [2] of SDN are discussed below:-

a). ORCHESTRATION:- Orchestration simply refers to the Automation. Software Defined Networking(SDN) has got the ability to run multiple number of devices with the help of certain commands. Orchestration in SDN simply means How you will coordinate various software actions with an centralized controller. The best way to built this is using Open Source Technology like Open Daylight. The main objective of this feature is capability to monitor the network and also automate connectivity. The prominent feature which SDN gives us is Automation with which the Services can be provisioned in a quick time and also reduces human error.

b). Centralized Control:- This feature of SDN is called as the basic feature of SDN which provides us a centralized control known as "SDN CONTROLLER". The SDN controller is logically centralized component but physically it is a distributed controller component. This controller provides a global view of the network and the whole network just looks like a single logical switch to the applications. With the help of SDN, network administrators can handle and control the whole network automatically and also dynamically from a single logical point, which simplifies the network operations and design as well [2]. Centralized control is very beneficial in case of distributed networking scenarios as well[13].

c). Abstraction and Virtualization:- One of the prominent benefits of a Software defined networking (SDN) is that it hides the complexity of the data flow in the network. Basically it hides the complexity of a network from applications by providing logical view of the network resources available and abstracting the actual traffic-flow control logic[13]. The Abstraction and Virtualization of resources helps us in making the network secure and also hides its complexity. SDN uses network resources without worrying about the fact that where they physically reside. In case of network devices like switches, routers, firewalls etc it is possible to divide them into different networks like making VLAN's or simply virtual networks. In SDN it is important to implement distinct/unique programming logic on these networks in order to attain security.

d). Programmability:- The important point which we conclude from studying about SDN is when comparing to traditional networks the SDN separates the control layer and infrastructure layer devices. The main objective of Programmability feature is to simplify the forwarding devices and also allows the networking software present in the SDN controller to evolve independently. So with the help of this we can attain a great potential in order to adopt best possible solutions. SDN provides us an easy and efficient ways to write immediate program logic for controlling the data-flow dynamically. In case of traditional networking, network devices like switches, routers etc., compute the best path for traffic flow by its own. Hence with the help of good programmability the speed of data flow will increase and there will be the reduction of latency inside the network devices.

e).Rapid Innovation:- we all know that 50% of business firms get involved in Open Source because it allows them to innovate. Software Defined Networking (SDN) helps in the deployment of new services. As far as the current traditional networking devices are concerned, the services has been embedded there simply with the hardware[13]. But the important point which needs to be taken into consideration is that these devices perform a number of operations like path computation, management of available resources in an optimal manner, Construct efficient paths etc. by itself. So the deployment of new application is limited to the services that came embedded with the hardware. However in case of SDN, the decoupling of the Infrastructure layer and Control layer allows us to attain the rapid deployment of unlimited services as networking devices only perform packet forwarding.

f). *Open Source Technology*:- Software Defined Networking (SDN) provides Open Hardware, APIs, Open Source Software, Open Standards with which we can determine the openness. The APIs basically act as tools in order to create software applications and they also tells us how different software components communicate with one another. Some of the important examples of all the above mentioned benefits which comes under openness are Open Flow Protocol, Open Networking Foundation(ONF), Open Stack and Open daylight, Open Compute Project etc. are working dedicatedly towards SDN. Open Flow is an important protocol that design many net-work switches in order to provide the communication between the centralized controller and the rest of the devices present in the network. with this important protocol i.e., Open Flow the centralized con-troller can decide the path of network packets through the network of switches and with the help of open programming API's network administrator can write the control-logic of traffic flow according to its own infrastructure requirement [41]. Openness is one of the prominent features of SDN because it allows anyone to participate let's take the example of Open Daylight. SDN has got the ability to undergo modification. In other words we say that openness allows flexibility and also the rapid growth of new networking techniques.

From the above mentioned features we conclude that the separation of planes and the various features of SDN makes it an efficient technology which is going to be the future of networking. Basically The importance of SDN lies in its characteristics/features discussed above as it provides flexibility by programming the control, including the centralized control, which helps in the management of a network. It becomes more valuable in case of distributed SDN networks working in synchronization. Also it is helpful in controlling, providing scalability and management of data in large data centres.

IV. SECURITY THREATS TO SDN

Software Defined Networking was developed in an attempt to simplify networking and make it more secure. By separating the control plane (SDN Controller)—which decides where packets are sent—from the data plane (Infrastructure layer/ physical network)—which forwards traffic to its destination, The SDN makers actually think that there is a possibility that we can achieve scalability and agility in network management. The application layer (virtual services) is also separate. Despite this new emerging technology provides us so many benefits but at the same time has got security issues as well. The security within the SDN is a big challenge right now as so much of work and research is being done in this field. As far as the security challenges in SDN are concerned they completely differ from the traditional networks because both the approaches differ in terms of the implementation and unique characteristics. Our current knowledge on SDN security issues are limited. In Software Defined Networking (SDN) architecture, the Control layer is separated from the infrastructure layer and is implemented in a software application. In this section we will mostly focus on the security issues with respect to SDN because of this separation. In the SDN architecture, the control layer, i.e., the Open Flow controllers, and its security have a direct impact on the data forwarding layer[14] . Since SDN Controller is the brain of the SDN architecture so it becomes the main component in the SDN architecture. The reason behind this is that it is responsible for the data flow occurring in the infrastructure layer. If this key element can be compromised the whole network is affected. This is because if a switch cannot receive forwarding rules from the controller, it will not know how to forward packets. Hence, due to its important role, the controller may become a key target for attackers, then the attackers can disrupt the data paths, they can modify the code and also change the script of traffic flows as well. The another important aspect which also should be taken into consideration is the communication between the Centralized Controller and the network devices residing in the data plane, they can also be exploited in many ways like:-

- Attackers can Install malicious Centralized controller and can to malicious information to the underlying SDN devices in the Infrastructure layer.
- Man in the middle attack for communication between the controllers and the SDN devices to change the instruction sent by the trusted controller[15].
- Attackers and Hackers may also install different types of security applications on the controller's northbound interface, with this they can open up new different ways to apply security policies on a entire network.

The above mentioned vulnerabilities may launch the most devastating attacks i.e., DOS attacks on the network devices residing in the infrastructure layer and they are capable of changing the path of information and also modify the code, changing the script as well to get access to the sensitive information. The multiple solutions has been so far given in order to mitigate these security issues in SDN architecture. Now we will address the other security threats of SDN and will discuss the counter measures surveyed so far that How actually these threats can be removed in SDN ?

4.1 Denial Of Service(DOS):- Denial of service(DOS) attack is one of the severe security threats to any type of network. This security threat decreases the performance of the whole network. Basically the Denial of service(DOS) attack increases the delay and also drop authorized packets as well as the Frames. It may also lead to disable the whole network or stop functioning. In Software Defined Networking(SDN), we know that there is a continuous flow between the SDN controller and the network devices like Routers, Switches etc, residing in the infrastructure layer of the SDN architecture due to which these network devices can attract the Attacker to move forwards their flow between them and interrupt the network activity [16]. We know that Denial of Service(DOS) is a flow level resolution attack, the information about the traffic flow is basically used to determine such type of security threats. Basically we use the flow based detection system that depends on the flow header which is present at the flow level. It has the large unbalanced traffic, “Fan-In” and “Fan-Out” where most of the traffic is going in a single direction [40]. The main challenge in detecting DOS attack is to differentiate the normal packet and the forwarding packet.

SDN networks contain various types of DOS attackers which needs to be addressed that is,

- **Switch DOS[Attack on forwarding plane/Data plane]:-** The network devices which we use in SDN like switches, routers, firewalls etc comprises of a restricted storage capacity and rely on the flow rules framed by the centralized controller. It is not possible to store all the flow rules in network devices like switch, router etc. So a special type of mechanism is used for this called cacheing mechanism, so that the flow rules will match with the incoming packets [40]. If a packet is not in cache it simply queries SDN controller. Once the flow rule is received, the packet is processed. This mechanism will make devices vulnerable to DOS attacks. The solution for this is we perform proactive cacheing, where network devices like switches, routers etc do not wait for receive packets, but cache a priori as many flow rules a table can fit [40].
- **Distributed DOS [Attack on control plane]:-** In Software Defined Networking (SDN) the Control layer is the most vulnerable to this security threat as multiple number of hosts distributed in the network may overflow. Since we know that all the flow rules are not already available in switches, so multiple number of queries are generated to end up processing power for legitimate users [39]. The solution for this problem is we perform "Replication" so that we can mitigate such attacks, where multiple controllers can manage the network rather than a single one [17], [39].

- **Spoofing:-** Spoofing and Sniffing are the two similar terms used in network security. The Sniffing simply means copying the information or modification of data while it travels from source to destination and Spoofing simply means deceiving computer devices, network devices or a user by an Attacker or Hacker on a network in order to launch attacks against network hosts, steal information, by-pass access controls, modify data etc. The main function of this security threat is that, it transmits traffic to the authorized hosts and can be eliminated by using proper authentication schemes. In simple words we say that Forging network information like IP, MAC, ARP to hide actual identity of traffic originator is known as spoofing [40]. In SDN the two most popular are IP spoofing and ARP Spoofing. We use ARP(address resolution protocol) for resolving MAC address to IP address. It basically take over the traffic from original receiver such that legitimate user is being knock out from the network [40]. In Software Defined Networking (SDN), Address resolution mapping (ARM) module is used to track MAC address from authorized host or simply maps IP with the MAC. The Centralized Controller simply consults this ARM module and rejects unauthorized ARP response [40]. “SSL” ENCRYPTION is basically used to prevent ARP poisoning between SDN controller and switches in OPEN FLOW [20]. We can prevent ARP spoofing by using Anti-ARP poisoning switch application in POX OPEN FLOW CONTROLLE [20],[36].

As far as the concept of IP spoofing is concerned in the field of networking it is called as the originator of other types of security attacks, the best example is DNS tampering. In this type of security attack the IP addresses are changed in order to redirect traffic, illegitimate websites by manipulation with DNS directories etc [17],[40]. The Enforcement of strong password encryption methods is necessary In order to avoid such problems that may be very much effective, it is necessary to implement the best encryption methods possible, like strong password encryption methods to avoid such issues. Also IP address verification method is also used to counter it. The two important ways are ”SAVI”(source address validation improvement) is a standard formalised by IETF which is used to verify addresses of packets [19], [40]. “VAVI”(virtual address validation edge) is extension of SAVI and based on OPEN FLOW. VAVI is simply embedded in SDN controller that verifies address of external packets that have no record in the flow table [19],[40].

4.2 Security Threats to the application layer and its countermeasures In SDN.

In case of application layer, the attackers main goal is to make unauthorized alterations in the network configuration, They also try to steal important information from the network, They may also take the network resources and try to introduce and spread out Viruses, Malicious computer programs etc to the application. In this way, they can obstruct the normal operation of the control layer and may also effect the reliability and availability of the network. One of the prominent protocol i.e., Open Flow can establish security detection algorithms for security applications in case of Software Defined Networking(SDN), these security applications are not mandatory [21]. The variety of applications developed by Different independent organizations made a lot of applications by using different Mobile Network Application programming languages in order to produce interoperability, inconsistency or security policy conflicts. Some of the security issues that may incorporate in the Application layer of SDN and Actions with which these security threats can be removed are discussed below**:-**

According to [1] there is a lack of standardize security mechanisms in Software Defined Networking (SDN) applications which leads to various security threats. In order to eliminate these Security threats different individuals has given different opinions about the security mechanisms for SDN applications that causes Security problems. According to scientists it is important to establish trustworthiness between the SDN applications running on the Centralized Controller. Presently we have got various techniques with which we can test the devices residing on the network but not the best measures with which we can test the applications. One of the best way to counter measure this is using "ACCESS CONTROL". Access control solution in SDN is characterized by a constant change and is also susceptible of modification or in other words we say is Dynamic and also flexible. The policy of Access control is implemented in firewall as per modify the requirement in the controller [40]. There are many architectures proposed by different scientists for Access control. According to [22] one of the proposed model is the, Ethane SDN architecture. This proposed model simply allows network administrators to implement hosts control by fine grained access control policies. Basically it uses the flow based networks and the central controller [40]. Also the reference number [23] had discussed dynamic monitoring in SDN Access list. One of the prominent access control system called "Resonance" is connected directly with the real time monitoring, which accelerates cycle taking alert from getting information. Basically the main objective in this is to Improve enterprise network attack response capability and the proposed solution to this is Dynamic access control system for securing enterprise networks.

The another important aspect is using "SDN Policies". Basically the configuration and implementation of network policies are facilated automatically in SDN. But in case of traditional networks the network policies were embedded in firewall and also its Access list, SDN allows policies at different level of abstraction [40]. SDN being a new architecture and that too very much innovative offers a number of new challenges for the enforcement, understanding, inform, and also the evaluation of network policies by automatic tools with smallest amount of human interaction. The main aim of the policy language is simply to write the formal and semi formal policies, which bridges the two level of abstraction [40]. Several languages of policy language are as below:-

a) According to [24] a proposed flow based management language (FML) is used to express Access list for NOX controller. Basically it is based on a declarative logic language that is used for connection with database and this declarative logic language is called as DATALOG. Another important thing which is used to implement policy in order to reach the correct matching rule for the current flow is the Decision tree. The best thing about FML is that it will maintain the states related to the list of devices, users. The decisions in the Access control are purely based on the value of attributes [40].

b) According to [25] proposed Alarms are used to implement policies for specifying and managing paths. According to [40], It is flow based specification language in order to interact with OPEN FLOW flows. Basically It is used as an administration tool to enforce policy through controlling and routing traffic. It also add attributes to FML related to flow content which enables Access control and implementation beyond the data link layer and the network[40].

V. CONCLUSION

In this survey we found that the biggest advantage of this new innovative technology is the separation of layers that makes it efficient and is also supposed to be the future of networking. The significance of the Software Defined Networking(SDN) lies in its architecture and its features. The important features like Centralized control with which we can control the whole network, Automation which allows us to examine the network, reduces human error as well and connectivity becomes easy, Programmability which provides us the flexibility etc. There are still many areas which needs to be taken into consideration while making SDN an efficient technology in future like security of a Centralized controller, Protect the SDN controller, establishment of trust etc. is the main area of concern. Also openness of SDN increases the chances of security issues as attackers can write programs in order to forge the data of a network and many more areas where modification is required. while studying the concept of Software Defined Networking (SDN), we found SDN being a relatively new area of research, has got both advantages and disadvantages in terms of security. A lot of solutions are there in SDN development but some modified solutions played an important role also some good steps to make sure things are secure like make sure we trust all the applicants running on the network also make sure we have good security policies. We all know that how fast Cloud computing is emerging day by day and is having a measurable impact on business. In order to collaborate these two concepts i.e., SDN and Cloud computing more and more security challenges will come forward So it is important to make SDN secure as much as we can.

REFRENCES

[1] Open Networking Foundation. *Software-Defined Networking: The New Norm for Networks (ONF White Paper)*; 2012.

[2] M. H. Razaa, S. C. Sivakumar, A. Nafarieha, B. Robertson, “A Comparison of Software Defined Network (SDN) Implementation Strategies”, Elsevier Proc. of 2nd International Workshop on Survivable and Robust Optical Networks (IWSRON). Vol. 32, pp. 1050-1055, 2014.

[3] M. Caesar, D. Caldwell, N. Feamster, J. Rexford, A. Shaikh, J. van der Merwe “Design and Implementation of a Routing Control Platform”, ACM Proc. of NSDI, Vol. 2, pp 15-28, 2005.

[4] P. Goransson, C. Black, “WHY SDN”, Software Defined Networks- A Comprehensive Approach, pp. 21-35, 2014.Y. Ding, J. Crowcroft, S. Tarkoma and H. Flinck, “Software defined networking for security enhancement in wireless mobilenetworks”, Computer Networks,(Elsevier) vol. 66, pp. 94 -101, 2014.

[5] J.Wan, C.Zou, K.Zou, R.Lu, and D. Li, "IOT sensing framework with inter-cloud computing capability in vehicular networking," Electron.Commerce Res., vol 14, no. 3,pp. 389-416, Nov. 2014.

[6] J. Wan, D. Zhang, Y. Sun, K. Lin, C. Zou, and H. Cai, ‘‘VCMIA: A novel architecture for integrating vehicular cyber-physical systems and mobile cloud computing,’’ Mobile Netw. Appl., vol. 19, no. 2, pp. 153–160, 2014.

[7] J. Wan, H. Yan, Q. Liu, K. Zhou, R. Lu, and D. Li, ‘‘Enabling cyberphysical systems with machine-to-machine technologies,’’ Int. J. Ad Hoc Ubiquitous Comput., vol. 13, nos. 3–4, pp. 187–196, 2013.

[8] K. Lin, W. Wang, X. Wang, W. Ji, and J. Wan, ‘‘QoE-driven spectrum assignment for 5g wireless networks using SDR,’’ IEEE Wireless Commun., vol. 22, no. 6, pp. 48–55, Dec. 2015

[9] J. Wan, H. Yan, D. Li, K. Zhou, and L. Zeng, ‘‘Cyber-physical systems for optimal energy management scheme of autonomous electric vehicle,’’ Comput. J., vol. 56, no. 8, pp. 947–956, 2013.

[10] S. Wang, J. Wan, D. Zhang, D. Li, and C. Zhang, ‘‘Towards smart factory for industry 4.0: A self-organized multi-agent system with big data based feedback and coordination,’’ Comput. Networks., vol. 101, pp. 158–168, Jun. 2016.

[11] *(An ISO 3297: 2007 Certified Organization)* Vol. 2, Issue 11, November 2014
Copyright to IJIRCCE www.ijircce.com 6519 ,Review On Architecture & Security Issues of SDN Gagandeep Garg1, Roopali Garg2 Research Scholar, Dept. Of IT, U.I.E.T., PU, Chandigarh, India1Coordinator, Dept. Of IT, U.I.E.T., PU, Chandigarh, India2.

[12] J. Wan et al., ‘‘Software-defined industrial internet of things in the context of industry 4.0,’’ IEEE Sensors J., doi: 10.1109/JSEN.2016.2565621.

[13] VM. World., 2014 Conference Coverage.

[14] Shin S, Yegneswaran V, Porras P, Gu G (2013) Avant-guard: scalable and vigilant switch flow management in software-defined networks. In: Proceedings of the 2013 ACM SIGSAC Conference on
Computer & Communications Security, pp 413–424.

[15] www.informationsecuritybuzz.com.

[16] Principles and Practices for Securing SDN, January 2015, ONF TR-511.

[17] The Software Defined Networking Research Group Published by IEEE Computer Sociaty 1089-7801/13/$31.00,2013 IEEE.

[18] Taxonomical Modelling of Security Threats in SDN ,Jennial Hizver, Phd, BlackHat Conference, August 5-6,2015.

[19] Yao G, Bi J, Xiao P (2011) Source address validation solution with Open Flow/NOX architecture. In: 19th

IEEE International Conference on Network Protocols (ICNP), pp 7–12.

[20] Fonseca P, Bennesby R, Mota E, Passito A (2012) A replication component for resilient Open Flow-based networking. In: IEEE Network Operations and Management Symposium (NOMS), pp 933–939.

[21] Canini M, Venzano D, Peresini P, Kostic D, Rexford J (2012) ANICEway to test Open Flow applications. In: Proceedings of the 9th USENIX Conference on Networked Systems Design and Implementation.

[22] Casado M, Koponen T, Shenker S, Tootoonchian A. Fabric: A retrospective on evolving SDN. *ACM HotSDN* 2012.

[23] A. K. Nayak, A. Reimers, N. Feamster, and R. Clark, "Resonance: dynamic access control for enterprise networks," in Proceedings of the 1st ACM workshop on Research on enterprise networking. ACM, 2009, pp. 11–18.

[24] T.Hinrichs, N. Gude, M. Casado, J. Mitchell, and S. Shenker, "Expressing and enforcing flow-based network security policies," University of Chicago, Tech.Rep, 2008.

[25] J. R. Ballard, I. Rae, and A. Akella, "Extensible and scalable network monitoring using Open SAFE," Proc.INM/WREN, 2010.

[26] Caraguay ALV, Lopez LIB, Villalba LJG. Evolution and Challenges of Software Defined Networking. *IEEE Communications Magazine* 2012

[27] Patouni E, Merentitis A, Panagiotopoulos P, Glentis A, Alonistioti N. Network Virtualisation Trends: Virtually Anything Is Possible by Connecting the Unconnected. *IEEE SDN for Future Networks and Services (SDN4FNS)* 2013.

[28] Akyildiz IF, Lee A, Wang P, Luo M, Chou W. A roadmap for traffic engineering in SDN-Open Flow networks. *Computer Networks* 2014; **71**:1–30.

[29] Galis A, Clayman S, Mamatas L, Rubio Loyola J, Manzalini A, Kuklinski S, Serrat J, Zahariadis T. Softwarization of Future Networks and Services - Programmable Enabled Networks as Next Generation Software Defined Networks. *IEEE SDN for Future Networks and Services (SDN4FNS)* 2013.

[30] Cahn A, Hoyos J, Hulse M, Keller E. Software-Defined Energy Communication Networks: From Substation Automation to Future Smart Grids. *IEEE SmartGridComm 2013 Symposium - Smart Grid Services and Management Models* 2013:558–63

[31] Nick.McKeown, T. Anderson, "Open Flow: enabling innovation in campus networks", ACM SIGCOMM Computer Communication Review, Vol.38, 2008.

[32] Azodolmolky S, Wieder P, Yahyapour R. SDN-Based Cloud Computing Networking. *ICTON* 2013.

[33] Sezer S, Scott-Hayward S, Chouhan PK, Fraser B, Lake D, Finnegan J, Viljoen N, Miller M, Rao N. Are We Ready for SDN? Implementation Challenges for Software-Defined Networks. *IEEE Communications Magazine* 2013:36–43.

[34] Azodolmolky S, Wieder P, Yahyapour R. SDN-Based Cloud Computing Networking. *ICTON* 2013.

[35] Lombardo A, Manzalini AG, Riccobene V, Schembra G. An Analytical Tool for Performance Evaluation of Software Defined Networking
Services. *IEEE Network Operations and Management Symposium (NOMS)* 2014.

[36] M. Dabbagh, B. Hamdaoui, M. Guizani and A. Rayes. Software-defined networking security: pros and cons. Communications Magazine, IEEE 53(6), pp.73-79.2015. . DOI: 10.1109/MCOM.2015.7120048.

[37] I. Alsmadi and D. Xu. security of Software-defined networks: A survey.Comput. Secur.53pp.79-108.2015.. DOI;
http://dx.doi.org.ez
proxy.library.dal.ca/10.1016/j.cose.2015.05.006.

[38] A. Shieha. Application layer firewall usingopenflow.2014.

[39] C. Yoon, T. park, S. Lee, H. Kang , S. Shin and Z. Zhang. Enabling security functions with SDN: A feasibility study. Computer Networks 85pp. 19-35.2015.. DOI:
http://dx.doi.org.ez
proxy.library.dal.ca/10.1016/j.comnet.2015.05..005.

[40] https://www.slideshare.net/parasDuthatra/sdnsecurity-59836812.

[41] A survey on energy efficiency in software defined networks, Mehmet Fatih Tuysuz a , , Zekiye Kubra Ankarali , Didem Gözüpek , https://doi.org/10.1016/j.comnet.2016.12.012.