Cihan University-Erbil Scientific Journal (CUESJ)

Review Article

An Overview on Software-defined Networking and Network Functions Virtualization Security Orchestration in Cloud Network Environment

Israa T. Aziz[1]*, Ihsan H. Abdulqadder[2]

[1]Computer Center, University of Mosul, Mosul, Iraq, [2]Department of Computer Science, Cihan University-Erbil, Kurdistan Region, Iraq

ABSTRACT

Cloud networks are being used in most industries and applications in the current era. Software-defined networking (SDN) has come up as an alternative tool and mechanism to follow and implement in a cloud networking environment in place of the traditional networking approaches. This paper includes the security aspects of computer networking concerning the cloud networking environment and SDN. The security risks and vulnerabilities have been listed and described in this work, and the measures that may be adapted to detect, prevent, and control the same. The use of figures, diagrams, and codes has been done as applicable.

Keywords: Software-defined network, network functions virtualization, cloud, cryptography, distributed denial of service attacks

1. INTRODUCTION

Cloud computing is a type of internet-based computing in which the devices communicate and are connected over a network which is usually the internet. Communications and transactions take place over the network in the case of a cloud environment, leading to the introduction of many security risks and threats. Software-defined networking (SDN) is a technique that is followed under computer networking that allows the network masters and administrators to make use of automated tools and applications to dynamically control and manage the networks as per the changing business requirements. Orchestration of SDN is the programming of such required automated behaviors to support the business applications and services.[1] Network functions virtualization (NFV), on the other hand, is a data center and network that has been specifically built and set up to manage the virtual networks and services over the cloud. NFV orchestration is the mechanism that is required to set up cloud-based applications and services over the cloud. SDN has come up as an alternative tool and mechanism to follow and implement in a cloud networking environment in traditional networking approaches. The architecture that is implemented in SDN is illustrated in Figure 1. Where, SDN divided into three major planes by open network foundation (ONF), the architecture in SDN as follows: Data plane: In this plane, forwarding devices such as switches, routers are interconnected. Connection in this plane can be established by either wireless connection nor wired connection. This plane is responsible for data forwarding accordance to flow characteristics. Control plane: This plane acts as brain of the network since it has the global view of entire network. This plane is responsible to program data plane elements. Forwarding devices: These are hardware- or software-based data plane device. Major function of these devices is to forward the data packets as per forwarding rules. Here, on incoming packets, actions such as forward to specify port, drop, and forward to control plane are taken. Southbound interface: This is referred as instruction set of forwarding devices that are defined by southbound application programming interfaces (APIs). The interaction between control plane elements and forwarding devices is carried south through southbound interface. Northbound interface: This API is offered by network operating system to application developers. This interface acts as common interface for developing new applications. Management plane: This plane is often called as application plane in which set of applications that leverage the functions offered by the north interface.

Corresponding Author:
Israa T. Aziz, Computer Center, University of Mosul, Mosul, Iraq.
E-mail: israa_aziz@uomosul.edu.iq

Received: May 17, 2021
Accepted: June 3, 2021
Published: June 20, 2021

DOI: 10.24086/cuesj.v5n1y2021.20-27

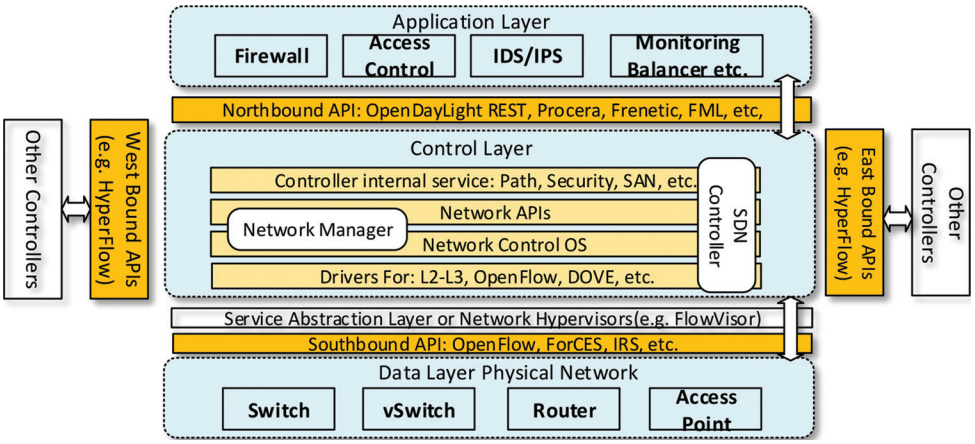

Figure 1: Software-defined networking architecture

Good design is the base of every software application and service. Therefore, it should be made sure that the software and the networks are constructed with the standard and necessary design patterns and principles. Figure 1 displays the various sets of interfaces and isolations present between the different layers of SDN that is either under evaluation or under development. For instance, the service abstraction layer (SAL) in the SDN architecture has been placed to isolate the APIs southbound from the controller. It would aid in the integration of the same controller with multiple APIs or protocols that are southbound. According to the software design aspects of SDN, the controller is the component that should make sure that the design is as per the flow insertion constraints and the entire network invariants are fulfilled before the insertion of a new flow rule in the process. Once the assurance is provided, a separate monitoring module shall be queried to retrieve the invariants.[2] Figure 2 depicts the characteristics that are associated with SDN. SDN is included with some security threats in data plane as well as in control plane.

Vulnerable Controller

In SDN, most of the network functions are realized in control plane by SDN controller. However, control plane is involved with some limitation such as queuing mechanism, security, and so on. SDN controller is responsible for network information collection, network configuration, and routing collection. If SDN controller is compromised or affected by attackers, this will be a massive attack held on SDN and network performance is degraded severely. In controller, well known denial-of-service (DoS), and distributed DoS (DDoS), target point-of-sale attack are frequently launched.

Risks Caused by Other Interfaces

Not only controller, in SDN, all other interfaces such as switches and gateways also affected by many attacks. SDN interfaces are programmable and open natured which leads probes attackers toward it. Attacks also held on application layer through northbound interfaces. Moreover, each layer in the network is affected by different attacks. Some attacking points in SDN are listed as follows,

- SDN switch – It is a separate device that is operated over OpenFlow (OF) protocol. SDN switch is also involved with flow tables which are limited in size

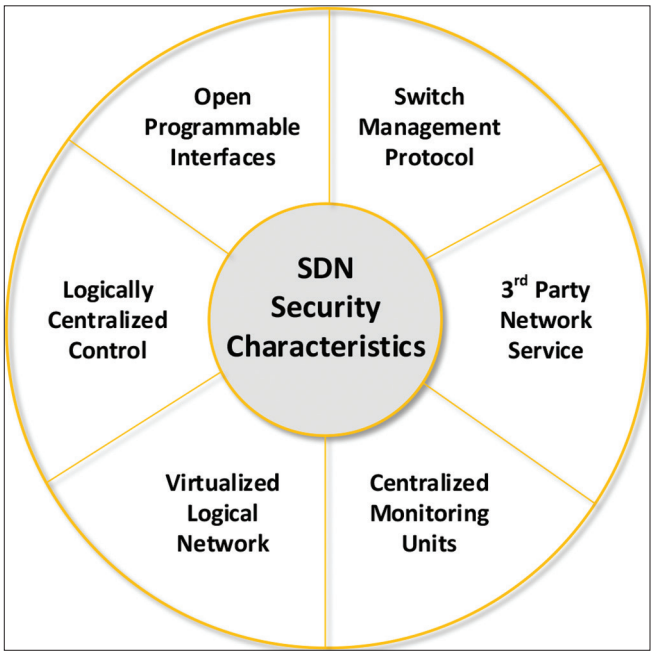

Figure 2: Software-defined networking characteristics

- Link between SDN switches – This type of attack is launched in SDN data plane in which link between data plane elements are targeted by attackers. In SDN, almost all data packets are transmitted between switches in the form of plaintext. This plaintext transmission in the data plane encourages the link spoofing attacks. Link between switches, controller, and switches-controller is also affected by man-in-the middle attack
- Link between SDN switches and SDN controller – This attack also launched as link spoofing attack in which link between controller and all switches is targeted by attacker. Remaining that all flow rules are installed on switches by controller through these links. Thus, this type of attack has high impact on the network
- Link between controllers –To support large number users, sometimes, the network is designed with multiple controllers. However, when multiple controllers are involved then attacking ratio also increased. Here, communication links between controllers also affected by attackers

- Application software – Usually, application software is built with controller on physical device. When this application software is affected by attacker, then it may inject malicious code to controller which destroys the entire network performance. Thus, application software is most convenient attack point for attackers. In application layer, unauthorized access also has major impact in the security point-of-view.

The primary characteristic that is associated with SDN is the logically centralized control. However, the same shall have the physically distributed controller component. A controller is a component that managed the complete network view of the associated infrastructure and also processed the entries based on the protocols as defined by the services and operations running above the same.[3] Another characteristic associated with SDN is the open programmable interfaces that have the major motivation behind them to permit the networking protocols implemented in the controller to execute and evolve independently. Furthermore, it makes sure that the forwarding devices are as simplified as possible. Switch management protocol, third-party network services, virtualized logical networks, and centralized monitoring units are also significant characteristics associated with the SDNs.[4] The rest of this paper is organized as follow, Section 2 presents the attack venders including the attacks in different layers. Section 3 provides the security threats and vulnerabilities in SDN. Section 4 illustrates different types of security measures while Section 5 concludes this paper.

SDN ATTACK VENDORS

SDN is a networking method in which virtualization is supported by the separation of the control plane from the forwarding plane. There are usually three layers in most of the SDN architectures, which comprise a lower layer in which network devices are placed, followed by the second layer, the middle layer in which controllers are kept. The topmost layer is the higher layer which consists of the applications and services to be configured as per SDN. The SDN is still in its early phases; however, the expansion of the same is quickly increasing, leading to the emergence and development of various security attacks by malicious entities. Several security threats and attacks have started to come up in association with SDN and the layers of the same. There are many attack vendors associated with these attacks, and the same has been explained as per the layers present in SDN architecture.

Attacks at Data Plane Layer

There are possibilities in SDN architecture that the attackers attack the network elements with the aid of the network itself. The basic technique that the attackers use in such cases is to gain unauthorized access to the network, which may be physical or virtual, and then give shape to the attacks. These attacks may be availability attacks such as denial of service attacks which have been explained in detail in the next section.

In SDN architecture, the controller uses several protocols to communicate and interact with other network elements. Some of the examples of such APIs and protocols include OF, embedded event manager, open management infrastructure, locator/ID separation protocol, and various others. These protocols comprise a secure mechanism within themselves to ascertain that the communications that take place over the network are safe and secure. Most of these protocols are relatively new, and there are high chances that there are security loopholes that may exist during the same implementation. These security loopholes allow the attackers to take advantage of the same and attempt to incorporate newer forms of flows in the flow table of the devices. There are spoofing attacks that are attempted to ensure that the local traffic is allowed over the network. There are malicious entities put up on the network for sniffing the same and performing unauthorized monitoring to gain relevant information through the act. Such attacks are termed as man-in-the-middle attacks in which an attacker sits on the network to gain information in an unauthorized manner. The attackers perform eavesdropping on the network flows to understand the flow of traffic over the networks.

Data centers are the prime spot of application for most SDNs. These data centers make use of several protocols in their functioning and operations, such as stateless transport tunneling, layer 2 multipath, shortest path bridging, and various others. All of these protocols comprise data packets which consist of data and information within them. The level of authentication in these protocols may not adhere to the required level to ensure secure communication. There are also instances wherein required encryption is not implemented in these packets. Therefore, these protocols may emerge as the attack vendors as they may provide the attackers with the opportunity to gain access to the network and information flowing over the network. There are several data integrity and availability attacks that may be executed due to these security loopholes.

Attacks at Controller Layer

After the data plane layer, the controller layer is present, and the middle layer is the target layer for the execution of several security attacks. There are several reasons behind the choice of the target as the controller layer by the attackers. If the attacker succeeds in spoofing the flows from the specific controllers, then the control of the traffic and the flows would come into the hands of the attackers. It would allow them to bypass the policies that may have been designed to enhance the security of the networks.

The attacker may execute various attacks to cause damage to the controller, and one such attack is the denial of service attack. There may be unauthorized consumption of resources that may be executed in addition to the deterioration of the frequency of packet transmission across the network. Such attacks would impact the network services and the flow of traffic over the network as well.

The controllers deployed in SDN architecture may be done in various operating systems such as UNIX or LINUX. The vulnerabilities associated with that of the operating system become the controller's vulnerabilities as well in such cases. There are issues with the deployment of the controllers in a production environment without strong passwords. Such vulnerabilities lead to weakening the network's security and allowing the attackers to execute several security attacks.

There are also instances in which the attackers create their controllers as per their set of policies and protocols and trick the network elements through the same. The network elements trust the fake controller as the original and various attacks are executed. There are malicious entries made into the flow tables which go undetected and unnoticed by the network engineers due to the nature of the controller. Such attacks are the worst forms of attacks as the attackers gain complete control over the network and gain an opportunity to turn the same in whichever direction they like.

Attacks at SDN Layer

Several attacks may be executed at the highest layer as the attacking vendor for the same. Attackers may attempt to impact the northbound protocol and its security. Many northbound APIs may be used in SDN architecture such as XML, Python, and Java. If the attacker succeeds in breaking through the security of a northbound API, the attacker would be able to gain control over the entire network with the aid of the controller. There are also chances wherein the attackers may create their own set of policies and launch them in the network to gain control over the entire environment of SDN.

There are also scenarios in which the default passwords of the APIs are not changed and used. In such cases, it becomes easier for the attackers to break into the network's security and execute various security attacks. It also allows the attackers to query the configuration associated with the SDN environment and alters the same to install their configuration in the network.

SECURITY THREATS AND VULNERABILITIES IN SDN

Information Breaches

Cloud networks deal with huge clusters of information that are passed from one source to the other. The exchange of information may involve a public cloud network, private cloud network, or likewise. The cloud network acts as a major threat agent, leading to the breaching of information by the attackers. These networks and the various access points present in the networks act as the source of entry for the attackers. They succeed in obtaining unauthorized access into the cloud networking environment.[5] The same leads to the violation of the viable properties of the information contained in the network, such as confidentiality, privacy, and the same availability.[6]

Information Leakage and Loss

SDNs also suffer from the loss or leakage of the data and information observed as one of the frequently occurring security attacks. When the information is passed from a source to the destination in the case of SDN, attackers get hold of the information bits and data sets which are then misused to cause damage to one or more parties associated with the same. The major threat agent, in this case, is the network and the networking protocols that are implemented. There are instances in which the information is prevented from reaching its designated destination, leading to significant damage.[7]

Malware Attacks

Malware attacks are the most common form of security attacks in a computing environment, and the case is the same with SDNs. The list of malware that can hurt the SDNs is a long one that comprises various types such as viruses, Trojan horses, worms, logic bombs, and many more. These malwares are also reproducible in most cases which makes it difficult to get rid of them. Therefore, it is required to adapt the measures to prevent malware attacks to ensure the safety of the network and the information contained within the same.[8]

Denial of Service and Distributed Denial of Service Attacks

SDNs introduce some advantages by decoupling the control plane from that of the data plane. However, the relationship between SDN and DDoS attacks is contradictory.[9] The capabilities and properties associated with SDN allow the detection of DDoS convenient and easy to execute. Simultaneously, the SDN architecture in which the control place of separated from the data plane gives rise to the newer forms of DDoS attacks. Such a property makes SDN a target of the denial of service and distributed denial of service attacks.[10]

The following is a basic DDoS script that the attackers may use in an SDN environment.

```
print "Attacking Mode is ON! ! ! ! ! ! ! ! !" + sys.argv[1] + "!
    ! ! ! ! ! !"
print "Injecting the Code " + sys.argv[2];
def attack():
#pid = os.fork()
s1 = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s1.connect((sys.argv[1], 80))
print "<<<<GET>>>>" + sys.argv[2] + " HTTP/1.1"
s1.send("GET/" + sys.argv[2] + " HTTP/1.1\r\n\r\n")
s1.send("Host: " + sys.argv[1] + "\r\n\r\n\r\n");
s1.close()
for i1 in range(1, 100000):
attack()
```

SECURITY MEASURES

DDoS Detection and Prevention

The most effective method which may be used to detect the DDoS attacks in SDNs is the fuzzy synthetic evaluation method. It is a method that has been developed based on fuzzy mathematics. With the aid of this method, the transformation is made from the qualitative method of evaluation to the quantitative method of evaluation. It is applicable for detecting DDoS attacks as it can evaluate the uncertainties with much ease and correctness.[11] The decision-making, in this case, is based on the three factors which areas listed below.

- Factor set F = {F1, F2, F3……. Fn}
- Judgment set J = {J1, J2, J3……Jn}
- Fuzzy relationship matrix R

There are also various flow checkers and flow detection mechanisms that may be used to detect DDoS attacks in SDNs.

Reduction of the Attack Surface

The control and reduction of the attack surface would prevent the security risks and attacks in the SDNs. These attack surfaces are the major threat agents that allow malicious entities to enter the network and impact the security and privacy of the information.[12] The network and data masters must ensure that the information exchanges that take place over SDN make use of smaller chunks of the data instead of larger data sets and pieces. Furthermore, the adaption of a secure APIs in the SDN architecture would lead to the prevention of the attacks in a private networking environment.[13]

Reduction of the Attack Window

Along with the smaller attack surface, the network administrators must also make sure that the attack window is reduced and brought out to the minimum. The reduction in the size of the attack window would significantly reflect the depreciation of the security threats and attacks. For example, there should be the use of rotating credentials in an SDN environment adapted by the network administrators.[14]

Use of Firewalls

It is necessary to maintain the initial steps of security in SDNs so that the attackers do not succeed in entering the network at all. Some of the firewall rules may be used in SDN, as Figure 3 described and listed below.

- At a particular switch, block the traffic from a specific host such as 11.1.1.1.
  00-00-02-00-00-00-00-00 BLOCK srcip=11.1.1.1
- At a particular switch, block the traffic that is coming from a specific host such as 11.1.1.2, if the particular packet say x TOS has been marked with 23 and it is required to be sent to the destination for 11.1.3.1
  00-00-03-00-00-00-00-00 BLOCK srcip=11.1.1.2 dstip=11.1.3.1 tos = 23
- At a particular switch, redirect traffic which is destined for 11.1.2.1 and, instead, send it to 11.1.2.2
  00-00-01-00-00-00-00-00 REDIRECT dstip=11.1.2.1 TO 11.1.2.2
- At a particular switch, mark the TOS field present in all the packets which are sent by 11.1.1.1 with a value of 42
  00-00-04-00-00-00-00-00 MARK srcip=11.1.1.1 TOS 42

Defense In-depth

This is the security measure that shall be used in SDN to prevent security risks and attacks. The interactions that are executed in a network are used in this security measure to prevent security attacks.[15] For example, a certain part or component of the SDN may get hampered by the security attack identified by another network and security part or component present in the architecture. These interactions between various components will ensure that the security of the overall network is maintained at all times.[16]

Cryptography and Encryption

Cryptography is a technique that comes under the advanced tools and techniques for preventing security attacks and enhancing information security. Encryption of the information is necessary in the present times with the introduction of so many security risks and attacks.[17] Cryptography is a phenomenon that makes use of public, private, or shared keys for the encryption of the information at the sender's end, which is then transferred in the same form and is decrypted with the help of the key at the end of the receiver.[18] Various encryption algorithms have been developed and may be used in the case of SDN security as well. One such algorithm is the Rivest, Shamir, and Adleman (RSA) encryption algorithm. For instance, the text required to be sent to the destination includes the bits "SDN." The encrypted form of the text is as specified below.

OIqsiWapHu0A3v93xxeUn+uTN2HxB8WKnl1
1ZZzj0xQaxGqKao63U4Qc8dnb2fow0Ls3uHRGo1VIL0Y
WcR8mPlZlxQ94dSRO1eK0yM0n0O5lqfUMZAsJ914gHI
ISkuk3mS/ZI+bs1zEqFGAJAb+yuPothtQ

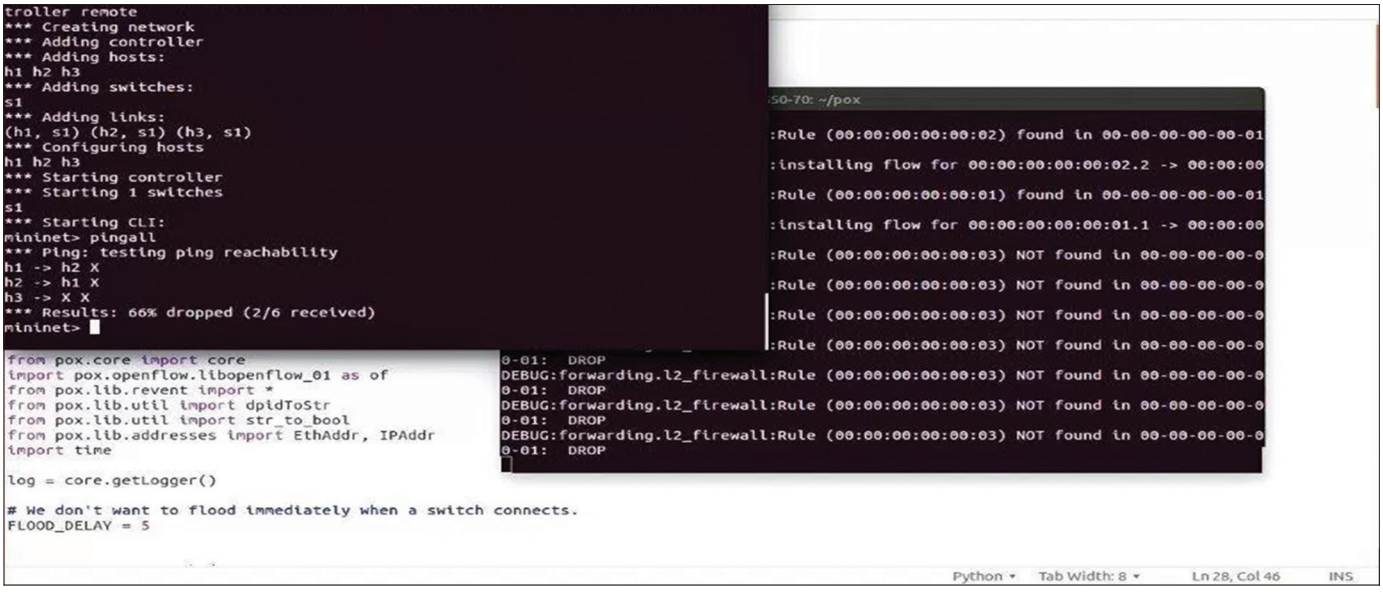

Figure 3: Firewall execution in software-defined networking

31RQHkR8ZqH9PGeTBlPN09rbvvzpPNxmI2G8g2DVug
B l W S x 0 a 1 Q j o V D Z w 8 t 0 0 v 7 9 Q h O c /
OqqA3TRMM6mjN5wMFISdUxnGtksKu7xlVMgms
FyEcZD6/9L7k2bpR3LlNuzxhlNqmRLxtnL8g4QIGwm
YQbe8i4pMWPtqImB1kqAkeE9dbpxNbLeNTEuwxw==

There is a private and public key pair used to encrypt and decrypt the information while the same is exchanged between the source and the destination over the software-defined network.

Various other encryption algorithms can be used, such as DES, triple DES, and many others. One of the widely used cryptographic functions is the SHA algorithm which stands for the single hash algorithm. SHA-256 is one of the forms of SHA that generates a unique 256bit hash for a text or data file, which is like a signature for the same.[19] For instance, the SHA-256 for the text "Software-Defined Network" is as specified as:

f8551cca082c82020b1f30b07a36a68c154272f9af16b
724859ccd1c96f64ae5

Access Management

Access to the information and data transferred and exchanged over the software-defined network is often played with by the attackers. The access points are used to gain unauthorized entry to the network. Therefore, it must manage access to the SDN using several administrative and technical security controls.[20] The administrative controls shall include enhanced security policies and protocols to control the access. In contrast, the technical controls shall include the use of technically advanced mechanisms such as multistep authentication, single sign-on, and likewise for the control of access.[21]

Advanced Tools

The number and frequency of data and network security attacks are on an all-time rise, and the same has led to the development of advanced tools and techniques for the detection and prevention of the same.[22] Therefore, it is required for the network administrators and masters to be constantly updated with the technical changes and innovations and adapt the advanced tools available in the market to prevent security risks and attacks. Various tools are now available for the management of the APIs, the execution of the security controls, and the management of the security attacks associated with the SDN traffic.[23,24]

Network Monitoring

Monitoring of the network at all times is also extremely important in the case of software-defined networks. Such a practice will ensure that there is no illegal activity across the network and the same is identified as soon as it is attempted.[25] The networking team shall carry out administrative practices such as networking audits, reviews, inspections, and non-stop monitoring of the network. Furthermore, there shall be automated intrusion detection and prevention tools that shall be implemented to ensure that the intruders do not get entry into the network.[26]

Network Monitoring Data Recovery and Backup Strategies

Electronic vaulting

Electronic vaulting is the procedure that incorporates the legitimate official of an electronic archive by keeping up the definitive duplicate of the same and the greater part of its associated and critical exchange reports in a protected area. The same is kept at the area until the lifecycle of the report is finished and accomplished. It is done keeping in mind the end goal to ensure that the electronically marked archive remains legitimately enforceable and allowable and accordingly frames an obvious review trail. Possession and consistency are resolved with this review trail as it were.[27] Electronic vault does not rotate around simply the capacity of the electronic archive additionally deals with the authorized access, support, and last demolition of the record. Aside from the legitimate and administrative edge, it likewise gives a protected move down to the available archive and opens electronically.[28] Certain components must be available in an electronic vault with a specific end goal to make it fit for its intended purpose. Electronic vault must make and give a great degree certain condition to the reports keeping in mind the end goal to guarantee the wellbeing, security, and protection of the information introduced in the archives. Exchange of records starting with one area then onto the next or starting with one vault then onto the next might likewise affirm the security highlights. Some archives do not permit the non-separated duplicates of the same to live in some other area separated from the electronic vault. Security of such records should be of most extreme confirmation as the loss of a unique copy will prompt losing the complete information related to the report. Electronic vaults must have an incredible system to keep up and deal with the duplicates of the electronically marked archives. The duplicates must have a personality or a stamping plan that separates them from the first record. There must likewise be instruments to track the entrance to the first e-archive or the duplicates of the same.[29]

Point-in-time copies

A point-in-time copy of an arrangement of information alludes to the copy of the information as it showed up at a specific period. It is a usable copy of the original information and has coherently happened at a specific timeframe. These copies might be perused just in nature or may give the compose capacities too. Various advantages accompany this alternative to move down the information[30] safely. It is frequently observed that while creating the move down on the cloud, the server is under a gigantic load. This regularly prompts a reinforcement window, which is hard to manage to keep the financial plan and timetable constraints in thought. The same is handled through the reinforcement alternative using point-in-time copies. The issue related to the open records additionally develops during the reinforcement. Clients continue updating the open documents till the last minute, and the go down of the same is not made. While creating the point-in-time copies, compose capacity of the record framework is not permitted, and consequently, the replication of the original archive or document is made. Point-in-time copies do not request specialists to play out the undertaking or recover the past renditions of the record, making it simple and a savvy

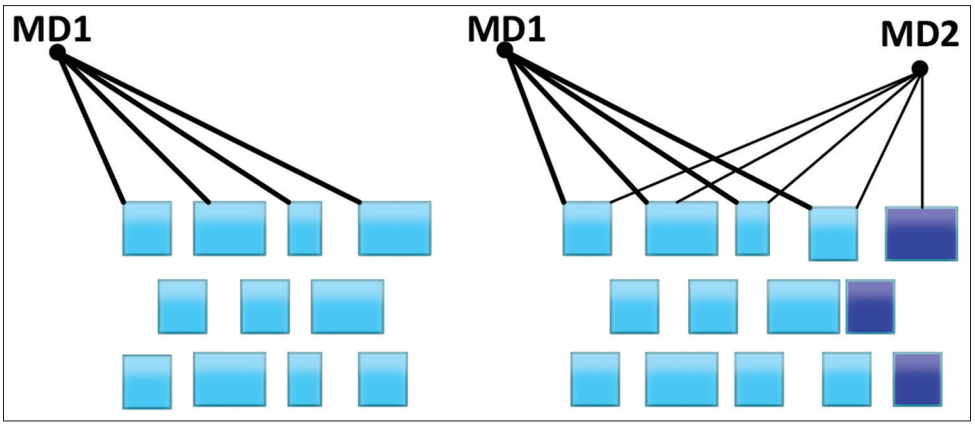

Figure 4: Data De-duplication methodology

arrangement. It is conceivable with the point-in-time copies to make the backup at constant intervals, generally impractical with the conventional techniques.[31]

Data deduplication

Information space available on the cloud is decreased with the assistance of data deduplication alongside giving the ability of information reinforcement. It ensures that the repetition related to the information is totally evacuated, and just a single duplicate or occurrence of the same is put away on the cloud. At whatever point a duplicate of information or repetitive information is discovered, it is indicated the first information. Because of its productivity to expel the excess information is also named as keen pressure or single occurrence stockpiling. Information deduplication joins the numerical calculations utilized as a part of the conventional pressure systems alongside delta differencing for looking at the old and new information and sparing just the bits of information that have changed.

Information deduplication makes the route toward reproducing fortification information practical by reducing the exchange speed and cost anticipated that would make and keep up duplicate informational indexes over frameworks. At a fundamental level, deduplication-enabled replication resembles deduplication-engaged information stores. When two photos of a support information store are made, all that is required to keep the generation or target undefined to the source are the infrequent duplicating and development of the new information divides, the general data deduplication methodology is shown in Figure 4.

Backup options

- Off-Site Cloud Backup – This is the backup option that may be used as a security measure in SDN security attacks to maintain know how of the entire data sets available on the cloud. Replication of the same ifs put away on the off-site location would be a wonderful option to ensure that the data can be recovered in the occurrence of an attack or a disaster
- Local Backup Options – With the presence of more than 1 storage option for the data and information present and exchanged in an SDN environment, it would be assured that the data are safe and protected at all times. The presence of a local backup option would be an excellent way to achieve the same
- Scalable and Easy to Use – Scalable backing up of the data is an easy and extremely cost-effective solution to ensure that the backing up of the data is convenient to use and execute as well
- DR Planning – Planning is always considered an effective measure for any of the activities, and the case is the same with disaster recovery.

CONCLUSION

The term SDN is a technique followed under computer networking that allows the network masters and administrators to use automated tools and applications to dynamically control and manage the networks as per the changing business requirements. Orchestration of SDN is the programming of such required automated behaviors to support the business applications and services. There are many security threats and vulnerabilities associated with the cloud networking environment in the case of a software-defined network, such as information breaches, data leakages, DDoS attacks, malware attacks, and many more. With so many security attacks, various security countermeasures are now available. They shall be implemented to ensure that the security risks and threats do not have any adverse impact and are prevented at all times. The most effective method which may be used to detect the DDoS attacks in SDNs is the fuzzy synthetic evaluation method. The control and reduction of the attack surface would prevent the security risks and attacks in the SDNs. These attack surfaces are the major threat agents that allow malicious entities to enter the network and impact the security and privacy of the information.

Along with the smaller attack surface, the network administrators must also make sure that the attack window is reduced and brought out to the minimum. Cryptography is a technique that comes under the advanced tools and techniques for preventing security attacks and enhancing information security. Encryption of the information is a necessity in the present times with the introduction of so many security risks and attacks. The same has proved to be effective in case of security attacks associated with SDNs. Other security measures that may be implemented include defense-in-depth, access management, firewalls, anti-malware, and many more.

REFERENCES

1. M. Gharbaoui, B. Martini, D. Adami, S. Giordano and P. Castoldi. Cloud and network orchestration in SDN data centers: Design principles and performance evaluation. *Computer Networks*, vol. 108, pp. 279-295, 2016.
2. J. C. C. Chica, J. C. Imbachi and J. F. B. Vega. Security in SDN: A comprehensive survey. *Journal of Network and Computer Applications*, vol. 159, p. 102595, 2020.
3. A. Shirmarz and A. Ghaffari. An autonomic software defined network (SDN) architecture with performance improvement considering. *Information Systems and Telecommunication*, vol. 2002, p. 121-129, 2020.
4. K. Nisar, I. Welch, R. Hassan, A. H. Sodhro and S. Pirbhulal. A survey on the architecture, application, and security of software defined networking. *Internet of Things*, vol. 2020, p. 100289, 2020.
5. D. M. Batista, G. Blair, F. Kon, R. Boutaba, D. Hutchison, R. Jain, R. Ramjee and C. E. Rothenberg. Perspectives on software-defined networks: interviews with five leading scientists from the networking community. *Journal of Internet Services and Applications,* vol. 6, pp. 1-10, 2015.
6. W. Li, Y. Wang, Z. Jin, K. Yu, J. Li and Y. Xiang. Challenge-based collaborative intrusion detection in software-defined networking: An evaluation. *Digital Communications and Networks*, vol. 7, no. 2, pp. 257-263, 2020.
7. A. M. Abdelrahman, J. J. Rodrigues, M. M. Mahmoud, K. Saleem, A. K. Das, V. Korotaev and S. A. Kozlovm. Software-defined networking security for private data center networks and clouds: Vulnerabilities, attacks, countermeasures, and solutions. *International Journal of Communication Systems*, vol. 34, p. e4706, 2021.
8. M. Rahouti, K. Xiong and Y. Xin. Secure software-defined networking communication systems for smart cities: Current status, challenges, and trends. *IEEE Access*, vol. 9, pp. 12083-12113, 2020.
9. S. Kunal, P. Gandhi, R. Sutariya and H. Tarpara. A secure software defined networking for distributed environment. *Security and Privacy*, vol. 3, p. e130, 2020.
10. B. Pinheiro, E. Cerqueira and A. Abelem. NVP: A network virtualization proxy for software defined networking. *International Journal of Computers Communications and Control*, vol. 11, pp. 697-707, 2016.
11. I. H. Abdulqadder, S. Zhou, D. Zou, I. T. Aziz and S. M. A. Akber. Multi-layered intrusion detection and prevention in the SDN/NFV enabled cloud of 5g networks using ai-based defense mechanisms. *Computer Networks*, vol. 2020, p. 107364, 2020.
12. P. K. Taksande, P. Jha, A. Karandikar and P. Chaporkar. Open5G: A Software-Defined Networking Protocol for 5G Multi-RAT Wireless Networks. In: *2020 IEEE Wireless Communications and Networking Conference Workshops* (*WCNCW*), pp. 1-6, 2020.
13. R. Etengu, S. C. Tan, L. C. Kwang, F. M. Abbou and T. C. Chuah. AI-assisted framework for green-routing and load balancing in hybrid software-defined networking: Proposal, challenges and future perspective. *IEEE Access*, vol. 8, pp. 166384-166441, 2020.
14. H. Zhang, Z. Cai, Q. Liu, Q. Xiao, Y. Li and C. F. Cheang. A survey on security-aware measurement in SDN. *Security and Communication Networks*, vol. 2018, p. 2459154, 2018.
15. L. Dong, L. Chen, B. He and W. Wang. The research on designs of multiple flow tables in the openflow protocol. In: *2018 27th International Conference on Computer Communication and Networks* (*ICCCN*), pp. 1-2, 2018.
16. K. Kondepu, C. Jackson, Y. Ou, A. Beldachi, A. Pagès, F. Agraz, F. Moscatelli, W. Miao, V. Kamchevska, V. Kamchevska, N. Calabretta and G. Landi. Fully SDN-enabled all-optical architecture for data center virtualization with time and space multiplexing. *IEEE/OSA Journal of Optical Communications and Networking*, vol. 10, pp. 90-101, 2018.
17. A. A. Barakabitze, A. Ahmad, R. Mijumbi and A. Hines. 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges. *Computer Networks*, vol. 167, p. 106984, 2020.
18. O. Yurekten and M. Demirci. SDN-based cyber defense: A survey. *Future Generation Computer Systems*, vol. 115, pp. 126-149, 2021.
19. R. Izard, J. Deng, Q. Wang, K. Xu and K. C. Wang. An agent-based framework for production software defined networks. *International Journal of Communication Networks and Distributed Systems*, vol. 17, pp. 254-274, 2016.
20. C. Zhang, X. Wang, Y. Zhao, A. Dong, F. Li and M. Huang. Cost efficient and low-latency network service chain deployment across multiple domains for SDN. *IEEE Access*, vol. 7, pp. 143454-143470, 2019.
21. L. Ben Azzouz and I. Jamai. SDN, slicing, and NFV paradigms for a smart home: A comprehensive survey. *Transactions on Emerging Telecommunications Technologies*, vol. 30, p. e3744, 2019.
22. S. Abdallah, I. H. Elhajj, A. Chehab and A. Kayssi. A network management framework for SDN. In: *2018 9th IFIP International Conference on New Technologies, Mobility and Security* (*NTMS*), pp. 1-4, 2018.
23. I. H. Abdulqadder, D. Zou, I. T. Aziz and B. Yuan. Validating user flows to protect software defined network environments. *Security and Communication Networks*, vol. 2018, p. 1308678, 2018.
24. M. H. M. Alhabib, M. Z. N. Al-Dabagh, F. H. AL-Mukhtar and H. I. Hussein. Exploiting wavelet transform, principal component analysis, support vector machine, and k-nearest neighbors for partial face recognition. *Cihan University-Erbil Scientific Journal*, vol. 3, pp. 80-84, 2019.
25. J. Bhatia, R. Dave, H. Bhayani, S. Tanwar and A. Nayyar. SDN-based real-time urban traffic analysis in VANET environment. *Computer Communications*, vol. 149, pp. 162-175, 2020.
26. V. P. Vladislav and V. P. Uliana. UPPAAL-based verification of software-defined networks. *Computing, Telecommunication and Control*, vol. 38, pp. 169-179, 2014.
27. R. Amin, M. Reisslein and N. Shah. Hybrid SDN networks: A survey of existing approaches. *IEEE Communications Surveys and Tutorials*, vol. 20, pp. 3259-3306, 2018.
28. R. Masoudi and A. Ghaffari. Software defined networks: A survey. *Journal of Network and computer Applications*, vol. 67, pp. 1-25, 2016.
29. Y. Afek, A. Bremler-Barr and L. Shafir. Network anti-spoofing with SDN data plane. In: *IEEE INFOCOM 2017-IEEE Conference on Computer Communications*, pp. 1-9, 2017.
30. W. Xiulei, C. Ming, W. Xianglin and Z. Guomin. Defending DDoS attacks in software defined networking based on improved shiryaev roberts detection algorithm. *Journal of High Speed Networks*, vol. 21, pp. 285-298, 2015.
31. P. Mishra, D. Puthal, M. Tiwary and S. P. Mohanty. Software defined IoT systems: Properties, state of the art, and future research. *IEEE Wireless Communications*, vol. 26, pp. 64-71, 2019.