International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

Common Vulnerability Scoring System for SDN Environment

Raktim Deb, Sudipta Roy

Abstract*: The identification of component vulnerability is an important criterion for securing the networks and it is an open issue for Software Defined Network (SDN). The First.org provides an open tool namely Common Vulnerability Scoring system for identification of component vulnerability, but there is no distinctive correspondence between CVSS and SDN. With this paper, we try to identify such correspondence so that it will help network researchers to determine the network vulnerability and improve the SDN security soon. This paper also includes a comparison between the last three CVSS versions. For this comparison, one can understand what are the new features CVSS incorporating for identifying new vulnerabilities in the emerging environment.

***Keywords* : SDN, OpenFlow, CVSS 3, Metrics Group .**

I. INTRODUCTION

The vulnerability of a system is nothing but the loopholes in the system that opens the door for the intruder to do malicious activity in the system. With the fast-growing demand for internet services, the estimation of the potentiality of any system is much required and important criteria to cope up with the demand. The Common Vulnerability Scoring System widely named as CVSS is an open support structure to quantify the severity of information system security vulnerability [1]. The CVSS provides the environment to the network manager to rank the severity of network component and rectify the loopholes beforehand it comes into action. The ranking is done based on three intrinsic group metrics such as a) Base group, b) Temporal group and c) Environmental group. Among these groups first, one rank the intrinsic characteristics and the second one identifies the individuality of a vulnerable component that alters over time and last one rank the features of each vulnerability that is distinctive to a corresponding user setting. Due to its wide viewpoint towards different features of vulnerabilities draws researchers mind for adopting CVSS. The researchers adopted CVSS in many environments like cyber security, network security, cloud security and more importantly SDN security also. But, no such elaboration has been mentioned that signifies one to one correspondence between the SDN components or properties to the CVSS metrics. We intend to identify and categorises SDN properties in contrast to CVSS metrics so that implementations of CVSS in SDN environment will be easier.

The outline of this paper is prearranged as follows. Section II describes the motivation and related works. In section III, a glimpse of CVSS is provided and section IV compares the last three versions of CVSS. Section V identifies the correspondence of CVSS and SDN properties. Lastly, sections VI conclude with uttering future work.

II. MOTIVATION AND RELATED WORK

With the fast escalation of the internet, sophisticated network vulnerabilities are been regularly discovered in the networking system. Consequences of such network vulnerability are that the vulnerability can be exploited and lead to stage network attack. The N Poolsappasit et al. in their research work uses CVSS ranking to estimate the attack probability when an intruder tries exploits common vulnerability at the first step of estimation and for more complex attack estimation they implement Bayesian attack graph [4]. Similarly to estimate the network security, the CVSS and Attack graph approach is adopted in [5, 6]. For cybersecurity assessment the authors in [7, 8] implement CVSS. M Aslam et al. introduces a security auditing and certification system namely ASArP which is also used CVSS for highlighting the impact of each misconfigured components of the system [9]. A smart grid represents the system of systems with coverage of diverse networking system to present the internet-based networking system. That means a smart grid is comprised of different unique components with different characteristics. Thus vulnerability identification of those components is an important criterion. In this respect authors J. Ko et al. introduces a novel quantification approach based on CVSS [10]. Like the smart grid, the cloud service providers also faced the security challenge due to the integration of different integration of unique components and API interoperability. Therefore suitable countermeasures much required for a cloud environment. In this respect authors K. A. Torkura et al. proposes a CVSS based probabilistic attack graph [11]. In another research work to assess the security risk of the cloud environment, the authors L. Maghrabi et al. propose a game-theoretic model where cost and benefit functions are based on CVSS [12].

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Raktim Deb*, Department of CSE, Assam University, Silchar, India. Email: debraktim@gmail.com
Sudipta Roy, Department of CSE, Assam University, Silchar, India.. Email: sudipta.it@gmail.com

The CVSS metrics are not limited estimating the vulnerabilities of networking devices or software's, it also is a standardized and consistent way to check the rigorousness of vulnerability of medical devices, clinicians devices also [13, 14]. Like other devices as mention in the section SDN devices are also not excluded from the adoption of CVSS. The authors B. K. Tripathy et al. propose a model for determining the threat value of each SDN components. In their threat model, the treat value is estimated by analyzing vulnerability and exposure in contrast to CVSS [15]. But this work does not provide the complete idea about one to one correspondence between CVSS and SDN entities. They took some relevant aspect of CVSS and implements in SDN domain.

The above discussion signifies the for any security assessment CVSS is widely adopted by the different field of the research domain and for the initial stage of estimation, CVSS is an important tool for the research workers. The authors P. Johnson et al. in their research work check the credibility of CVSS scorings based on five foremost databases (OSVDB, CERT-VN, NVD, X-Force, and Cisco) [16]. The outcome suggests that with the special case of some measurements, the CVSS is very dependable.

The SDN is emerging technology and its security issues are in current trends in the research domain. Therefore identifying the correspondence between CVSS and SDN properties is much required for security concern. Such correspondence will help researchers to do well refine security research in SDN domain. This visualization motivates us and identification of such correspondence is the prior concerns of this paper. The next section will provide an eye blink idea about the CVSS 3 and a comparative idea with the previous version.

III. CVSS FRAMEWORK

The CVSS is one of the most popular, common and widely accepted frameworks to assess the vulnerability of the IT system. The US National Infrastructure Assurance Council (NIAC) was the first organization produced CVSS in 2005 [3]. Now the Forum of Incident Response and Security Team (FIRST) is the custodian authority of CVSS for future improvement. The FIRST produced CVSS version 3 in 2015 which is more refined and improved version compare to previous versions. In this section we cover a formal discussion about CVSS 3, what are new features it provides compare to previous version and reason behind choosing CVSS 3 for SDN.

The CVSS 3 is comprised of flowing group metrics

A. Base Metric:

This metric group identifies the intrinsic or fundamental independent individuality of vulnerable components that are explicit to the user environment. The Base metric is also subdivided by the three components that are.

- **Exploitability metric:** this metric captures the technical means to identify the characteristics of the vulnerable component that can be exploited using the following parameters:

i. **Attack Vector (AV):** The AV metric captures the circumstance by which the misuse of a vulnerable component is possible. It is assumed that the chances of exploitation from remote access are greater than physical access. Therefore, this sub metric category in four different categories which are: Network, Adjacent Network, Local and Physical. Among these four category network has the maximum score and Local is minimum.

ii. **Access Complexity (AC):** The AC metric describes the measurable amount of effort that is a prerequisite to accomplishing the successful exploitation of a vulnerable component. This metric is categories in two different values which are: High and Low.

iii. **Privileges Required (PR):** The PR metric captures the context of privileges level that is required to accomplish the successful exploitation. This metric is categories in three different values which are: None, Low and High. The PR metric will represent high value if PR is None and vice versa.

iv. **User Interaction (UI):** The UI metric describes the scene to accomplish the exploitation of a vulnerable component user interaction, other than the attacker is required or not. This also categories in two different value which are: None and Required. The None value is represented as the greatest concern among the two.

- . **Scope (S):** It is an important property introduced in CVSS 3 and represents the measures of scope for a vulnerability that can activate an alteration of access permission in the targeted networking architecture. It has categories into two values which are: Unchanged and Changed. The changed scope means that the access permission of one vulnerable component can take the privilege of access permission of any other component in the system.
- **Impact Metrics:** This metric characterized the consequences of an impacted vulnerable component such that exploited component is affecting the security measures: Confidentiality, Integrity, and Availability of a system or not.

B. Temporal Metrics

This metric represents the measure of the individuality of the vulnerable component that alters over time. It identifies the present status of code availability or exploitation techniques or the level of assurance regarding the technical details of the existing vulnerability. This metric is subcategories into three parts which are: Exploit Code Maturity (E) - probability measures of vulnerability being exploited, Remediation Level (RL) – prioritization of unpatched vulnerability and proving the solution, Report Confidence (RC) –the level of assurance regarding the existence of the vulnerability and available technical knowledge.

C. Environmental Metrics

This metric characterizes the vulnerabilities that are allied with a particular user's environment and refines the base metric rankings, based on certain environmental understandings.

The CVSS metrics that are mentioned in this section contribute rankings in the range of 0-10. Also, these metrics can be represented as textual format, known as vector string. For example: AV:AN / AC:L / PR:L / UI:R / S:U / C:L / I:L / A:N is a vector string, means that while ranking the score the system consider Attack Vector is Adjacent Network, Low Attack Complexity, and Privileged Required, User Interaction is required, Unchanged Scope, Confidentiality, and Integrity is Low, and Availability is None.

IV. COMPARISON BETWEEN CVSS 3 AND ITS PREVIOUS VERSIONS

After a long-standing effort of Special Interest Group (SIG) of FIRST.org introduced the CVSS version 3 was introduced in 10th June 2015. This version refines the shortcomings of CVSS version 2 and version 1 and provides the metric values that are very close to real-life requirement while ranking the vulnerable components. This section identifies the shortcomings of previous versions and describes the refinements of version 3 concerning these shortcomings. The categorization of CVSS metrics is almost the same in every version but each version comes with few refinements.

The first generation CVSS Access Vector sub metric suffers from differentiating between the remote network vulnerability and local network vulnerability. The SIG also identifies the discrepancies in access vector and proposed three new values which are Local, Adjacent Network and Network in version 2. Version 3 introduces more refinement in the access vector by adding one more value namely Physical. The Physical value identifies the vulnerability which requires the attacker to physically access the resource for exploitation.

The authentication sub metric suffers from differentiating in the identification of a single step or multiple step authentications for the system. Therefore, to make identification more accurate SIG proposes three metric values in version 2 which are: None, Single and multiple [2]. Later SIG identifies that only providing authentications at a granular level is not sufficient to cope up with the fast-growing internet. Therefore the SIG changed Authentication metric to Privileged Require with values of None, Low and High and one more additional sub metric User Interaction with values None and Required is introduced in version 3.

Version 3 introduces a new sub metric namely Scope into the Base metric category. The metric value of Scope is: Changed and Unchanged. The changed value signifies that vulnerability in a component, rather than impact itself it might impact the other component in the system. The unchanged value signifies that vulnerability of a component impacts itself only.

In the last two versions the Impact Metrics: Confidentiality, Integrity, and Availability are a measure of severity impact independent vulnerabilities. So the value of C, I, A is None, Partial and Complete. By the introduction of Scope sub metric now CVSS is capable of taking consideration of vulnerable component interaction. Therefore the valued of changed to High, Low and None.

Lastly, the Environmental Metric is refined and a new sub metric Modified Base Metrics is introduced in version 3. This sub metric provides freehand to the system analyst to modify the Base metric in following their system requirement. Therefore the system analyst set the base metric especially Integrity metrics in such a way that difficulty level of exploitation of vulnerable component will increase. The default numerical value of the Base metrics and the Modified Base Metrics are the same numerical unit. The above comparison is represented in Table I.

The CVSS version 3 [1] is not only a more refined version among the previous versions it also provides the capability to rank the vulnerability of the computing resources in real-time aspects. Therefore any emerging computing environment like SDN needs a distinctive idea about CVSS implementation in the respective environment. The prior goal of this paper is to represent the distinctive idea about CVSS implementation in SDN and is discussed in the next section.

V. CORRESPONDENCE BETWEEN SDN PROPERTIES AND CVSS 3

The SDN is an emerging technology in the networking environment and an interesting domain for networking researchers. The SDN brings the new architectural view in networking environment as well as new challenges also. Among the many challenges network security is the prior concern for the researches. Thus understanding the CVSS concerning SDN environment will help improve network security research and increase the chances of proving more refine networking mechanism.

The SDN brings new perception in network control by separating the control plane from the data plane, proving centralized control to the network and providing open programmability in the network. Not only that the perception of networking communications is also new. In SDN environment a network communication will hold only under the supervision of control plane i.e. when a request comes from end host to the network switch namely OpenFlow switch, the OpenFlow switch will send information to the control plane by sending Packet_In message. The control plane decides the request and instructs the Openflow switch how to deal (forward/drop) with the request. The communication mechanism is shown in figure 1.

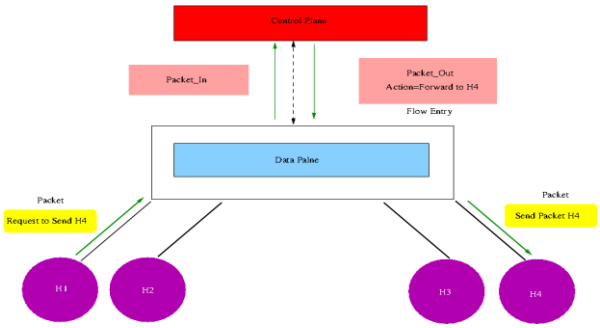

Fig. 1.SDN Communication Mechanism

Table- I: Comparison between CVSS versions

CVSS Version 1		CVSS Version 2		CVSS Version 3	
Base Metrics					
Attack Vector/ Modified Attack Vector (for Version 3 only)					
Metric value	**Numeric value**	**Metric value**	**Numeric value**	**Metric value**	**Numeric value**
Local	0.7	Local	0.39	Local	0.55
Remote	1.0	Network	1.0	Network	0.85
		Adjacent Network	0.646	Adjacent Network	0.62
				Physical	0.2
Attack Complexity/ Modified Attack Complexity (for Version 3 only)					
High	0.8	High	0.35	High	0.44
Low	1.0	Low	0.71	Low	0.77
		Medium	0.61		
Privilege Required/Modified Privilege Required (for Version 3 only)					
Authentication		**PR**		**PR/MPR**	
Required	0.6	Multiple	0.45	High	0.27/50 if Scope Changed
Not Required	1.0	Single	0.56	Low	0.62/0.68 if Scope Changed
		None	0.704	None	0.85
User Interaction/ Modified User Interaction					
				None	0.85
				Required	0.62
C, I, A Impact/ Modified C, I, A Impact (for Version 3 only)					
None	0	None	0	None	0
Partial	0.7	Partial	0.275	Low	0.22
Complete	1.0	Complete	0.660	High	0.56

To process the request the OpenFlow switch maintains a flow table and stores the request information. If flow request information is already in the flow table than a switch does not require granting permission from the control plane, switch itself capable process it. These features increase the flexibility and adaptability of the network compares traditional architecture.

The SDN features might use to increase flexibility, adaptability in the networking environment compare to traditional network but it also possesses vulnerability in the component as well as in the communication mechanism. In this paper, we intend to distinguish the SDN vulnerability in contrast to CVSS.

A. Base Metrics

This metric is comprised of three sub metrics such as a) Exploitability metrics b) Scope and c) Impact Metrics

- **Exploitability Metrics:** again the Exploitability metric is subdivided by following metrics

i. **Attack Vector:** this sub metric represents the existing path by which exploitation is possible to the SDN network. Attack vectors comprise of four metric values: Network, Adjacent Network, Local and Physical. To identify these entire metric values figure 2 is represented. Figure 2 signifies the existence of all these metric values in the SDN network. The blue dotted line shows a possible scenario for Network attack vector, green dotted line for Adjacent Network, and grey dotted line for local.

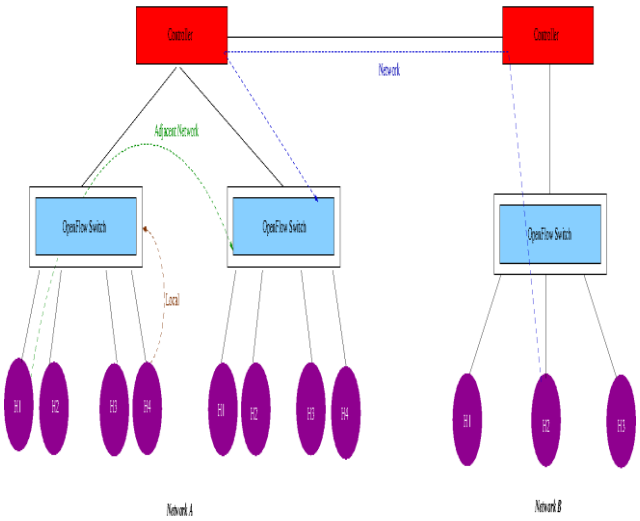

Fig. 2. Possibe Attack Vectors

ii. **Access Complexity:** this sub metric represents the efforts or prerequisite needed to achieve exploitation of network component. The SDN provides a global view of network therefore; any network application can able to access any component of the network. Not only by default data plane and control plane communication is asynchronous communication. In default SDN there transport layer security is implemented. It suggests access complexity is low in SDN by default. The access complexity is high only when if a mechanism is implemented in the network and an attacker needs some preparation to generate exploitation in this circumstance. For example, ROSEMARY [17], PANE [18], LegoSDN [19] are a few SDN control plane where access complexity is high.

iii. **Privilege Required:** it represents the rights to access any component in the network. The SDN provides open programmability in the control plane or control plane applications. Not only that the global view feature of SDN provides access permission for each component in the network. This simply means that there is no authentication mechanism in the control plane. Further, the Data plane and control plane is not synchronous. Both conditions signify that by default SDN architecture Privilege Required is low. SDN controller like ROSEMARY [17], PANE [18], LegoSDN [19] where privilege required is high.

iv. **User Interaction:** this metric describes the circumstances were to generate exploitation user interaction is required or not. Both the conditions are true for SDN architecture. As SDN control plane application gets the chance of a global view of the network and open programmability features is available in the control plane, any malicious applications or malicious code in the applications can able exploit the network component with intervening the user. Another scenario, in the data plane, uses asynchronous communication with the control plane. Therefore any malicious end-user can also be capable of generating the exploitation in the network. The above discussion signifies that both metric values (Required and Not required) are applicable in the SDN architecture.

- **Scope:** this metric determines that exploitation of any vulnerable component is impacting other components or not. This metric is included in CVSS 3 for the first time. In SDN architecture very much required aspect as SDN component is correlated to each other. For example, if the control plane is vulnerable than it will impact the whole network. If the control plane application is vulnerable then it might impact OpenFlow switches in the network or end host in the network or control plane also. If OpenFlow switch vulnerable then it might impact control plane or end host or any adjacent network also. Therefore, both scope change and unchanged metric value are important for the SDN network.

- **Impact Metrics:** this metric is comprised of confidentiality, integrity, and availability of the components.

i. **Confidentiality:** is deal with the vulnerability that impact network configuration or network communication. The confidentiality metric identifies the vulnerability of a component that leaks the network information for which exploitation is conceivable. In SDN data communication is asynchronous and information passes during communication use plain text messages. Not only that the incoming packet handling mechanism also leaks the network information as processing time of input packets that arrived for the first time is different from the second packet or other packets. This tap gap occurred due to control decision makings for handing the packets and by sincere looks on network activities, an attacker can easily identify the current state of network configuration. Therefore by default confidentiality is High in SDN. The SE-Floodlight [20] or FortNox [21] based control plane implements security patches by default, therefore such control plane can make confidentiality of SDN near to None or Low.

ii. **Integrity:** is deal with the vulnerability that impacts the trustworthiness of network configuration or network components. The SDN provides open programmability in the control plane and global view. Due to this facility any network programmer able to write own code or network functionality in the network. There may be chances those codes are vulnerable or a malicious programmer inject vulnerable in the control plane. Moreover, global view functionality is provided by the SDN to any application running on the control plane. Therefore, malicious users using the vulnerable code fetch the network component and able to do unfair activities in the network. Thus integrity is High in SDN control plane. There is no privileged checking for data plane components which is another reason for reducing the trustworthiness of SDN and making integrity metric value at High.

- **Availability:** is deal with the vulnerability that impacts the readiness of resources in the network. In SDN data plane a small amount of memory space is provided for storing flow table information. Thus there are chances of exhausting the memory space while maintaining the high amount of network traffic. If this circumstance occurred in the SDN the underneath end hosts will face the unavailability of network resources. Not only that there may be chances the exhausting the data to control plane path or control plane resources using malicious traffic flow. These circumstances have a devastating effect on the network as exhausting the control plane means making whole network communication unavailable in SDN. The above discussion means that the value of Availability metric is High in SDN.

B. Temporal Metrics

- **Exploit Code Maturity:** this metric describes the probability of vulnerable component is being exploited by the current state of exploitable techniques and exploitable code availability. The D Kerutz et al. in their research work [22] identify that there are 7 possible threats exists in SDN environment and among them, three are SDN specific and other four are similar to the traditional network. Therefore all four Exploit Code Maturity are applicable for SDN network.

- **Remediation Level:** this metric identifies the availability of fixes or patches for the vulnerability. In SDN some fixes are provided by the OpenFlow Specification like OpenFlow specification [23] introduces TLS implementation in the SDN architecture. Some other fixes still under the custody of research works. Thus all metric values are applicable in the SDN architecture.
- **Report Confidence:** this metric describes the level of confidence regarding vulnerability and technical knowledge. In SDN network some vulnerability like data to control plane communication, limitation in OpenFlow switch memory, missing user privilege is already identified. The SDN is a rising technology, thus new vulnerability will be identified day by day with the adoption of this technology. Therefore serious attention is much required while maintaining the report to increase the level of confidence for the SDN environment and all metric value will help in this regards.

C. Environmental

This metric is comprised of four sub metrics which are Confidentiality Requirement, Integrity Requirement, Availability Requirement, and Modified Base metrics. These metrics help SDN to tailor the importance of C, I, A sub metrics for the SDN vulnerable component compare to other metrics to reorganize the rankings. This metric is very much useful and must require criteria for SDN architecture, as the prioritization is required for the SDN control plane will be different from Openflow switch or end host. The control plane is the heart of the network if control plane compromised that it will affect the entire network but if a switch is it affects a subpart of the network. The scope change and privilege required metric have an adverse effect on the SDN environment. Therefore, Modified Base Metrics have an import rule while ranking the SDN components. This metric helps SDN to prioritize its components based on identified severity while implementing SDN in a particular domain. All the above discussion represents in tabular format in table II.

Table II provides a distinctive idea about the implementation of CVSS 3 in the SDN environment.

Table- II: CVSS Applied on SDN

Group	Metric	Metric value	Numeric value	Definition
Base	Attack Vector	Network	0.85	From any position of the network (Internal or External entities) of SDN
		Adjacent Network	0.62	From any Neighbor Network of SDN
		Local	0.55	Within the SDN
		Physical	0.2	Physical access to SDN components
	Complexity	Low	0.77	The condition that identified from SDN Specification
		High	0.44	Condition unknown
	Privilege Required	None	0.85	User privilege required
		Low	0.62/0.68 if Scope Changed	
		High	0.27/0.50 if Scope Changed	Control plane application, Data plane, end host or accessing any component privilege required
	User Interaction	None	0.85	Control plane application accessing the SDN Components.
		Required	0.62	End host trying to access the End host Component

	C, I, A	High	0.56	When malicious user capable of access the network component or network information and makes resources unavailable.
		Low	0.22	When information access is done by only authorized users and makes resources partially unavailable.
		None	0	
Temporal	Exploit Code Maturity	Not defined	1	If code is readily available to exploit the SDN components (vulnerable or not vulnerable) or SDN communication.
		High	1	
		Functional	0.97	When code is function only for the vulnerable components of SDN.
		Prof of Concept	0.94	When code is functional for the traditional network but not in the SDN environment.
		Unproven	0.91	When no exploitation mechanism is available.
	Remediation Level	Not defined	1	If the solution is not available for the vulnerability.
		Unavailable	1	
		Workaround	0.97	If the solution is available to the nonvendors.
		Temporary Fix	0.96	If a temporal solution is available to the vendor.
		Official Fix	0.95	If the complete solution is available to the vendor.
	Report Confidence	Not defined	1	When ranking is not influenced in the practical.
		Confirmed	1	When the document is available and vulnerability is proven in practical
		Reasonable	0.96	When the document is available and vulnerability is theoretic only, not proven in practical
		Unknown	0.92	When the document is available but distinctive causes are unknown for SDN environment.
Environmental	C, I, A Requirement	Not defined	1	When ranking is not influenced in the practical.
		High	1.5	When it is identified that loss of C, I, A catastrophic adverse effect in SDN.
		Medium	1	When it is identified that loss of C, I, A adverse effect in SDN.
		Low	0.5	When it is identified that loss of C, I, A limited adverse effect in SDN.

VI. CONCLUSION AND FUTURE WORK

The network researchers of the traditional network widely adopted CVSS to identify the existing vulnerability of network components before the implementation of their network. The adaption of CVSS makes network researchers confident enough about their network security. Therefore a clear cut understanding of CVSS is much required for SDN researchers also, to implement CVSS in SDN. In this paper, we identify the one to one correspondence of CVSS and SDN properties. This will help SDN researcher to implement more refine security mechanism in the SDN environment. But the problem with CVSS is that it does not specify the ranking for the mutual vulnerability of multiple components. In our future work, we will try to the mutual vulnerability of SDN components.

REFERENCES

1. CVSS Special Interest Group(SIG), Common Vulnerability Scoring System v3.0: Specification, FIRST.ORG, Inc., 2015.
2. CVSS Special Interest Group(SIG), Common Vulnerability Scoring System v2.0: Specification, FIRST.ORG, Inc., 2007.
3. National Infrastructure Advisory Council, Common Vulnerability Scoring System v1.0: Specification, FIRST.ORG, Inc., 2005.
4. N. Poolsappasit, R. Dewri, I. Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs," in *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 1, pp. 61-74, 2012.

5. L. Gallon, J.-J. Bascou, CVSS attack graphs, Proceedings of the Seventh International Conference on Signal Image Technology & Internet-Based Systems (SITIS 2011), IEEE, Dijon, pp. 24-31, 2011.
6. L. Muñoz-González, D. Sgandurra, M. Barrère, E. C. Lupu, "Exact Inference Techniques for the Analysis of Bayesian Attack Graphs," in *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 2, pp. 231-244, 2019.
7. M. U. Aksu *et al*., "A quantitative CVSS-based cyber security risk assessment methodology for IT systems," *2017 International Carnahan Conference on Security Technology (ICCST)*, Madrid, pp. 1-8, 2017.
8. L. Allodi, F. Massacci, Security Events and Vulnerability Data for Cyber security Risk Estimation. Risk Analysis, 37: 1606-1627, 2017.
9. M. Aslam, C. Gehrmann, M. Björkman ASArP: automated security assessment & audit of remote platforms using TCG-SCAP Synergies, Journal of Information Security and Applications, ISSN: 2214-2126, Vol: 22, Page: 28-39, 2015
10. J. Ko, S. Lee, T. Shon, Towards a novel quantification approach based on smart grid network vulnerability score. *Int. J. Energy Res.*, 40: 298– 312, 2016.
11. K. A. Torkura *et al*., Securing Cloud Storage Brokerage Systems Through Threat Models, *2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*, Krakow, pp. 759-768, 2018.
12. L. Maghrabi, E. Pfluegel and S. F. Noorji, "Designing utility functions for game-theoretic cloud security assessment: a case for using the common vulnerability scoring system," *2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security)*, London, pp. 1-6, 2016.
13. I Stine, M Rice, S Dunlap, J Pecarina, A cyber risk scoring system for medical devices. International Journal of Critical Infrastructure Protection, 19, C, 32-46, 2017.
14. M. P. Chase, Steven M. Christey Coley, Rubric for Applying CVSS to Medical Devices, Technical Paper, The MITRE Corporation, 2019, https://www.mitre.org/publications/technical-papers/rubric-for-applying-cvss-to-medical-devices.
15. B K Tripathy, D P Das; S K Jena, P Bera, Risk based Security Enforcement in Software Defined Network, Computers & Security, ISSN: 0167-4048, Vol: 78, Page: 321-335, 2018.
16. P. Johnson, R. Lagerström, M. Ekstedt and U. Franke, "Can the Common Vulnerability Scoring System be Trusted? A Bayesian Analysis," in *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 6, pp. 1002-1015, 2018.
17. S Shin, Y Song, T Lee, S Lee, J Chung, P Porras, V Yegneswaran, J Noh, B B Kang, Rosemary: A Robust, Secure, and High-performance Network Operating System, In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14). ACM, New York, NY, USA, 78-89, 2014.
18. A D. Ferguson, A Guha, C Liang, R Fonseca, S Krishnamurthi, Participatory networking: an API for application control of SDNs. SIGCOMM Comput. Commun. Rev. 43, pp 327-338, 2013.
19. B Chandrasekaran and T Benson, Tolerating SDN Application Failures with LegoSDN. In Proceedings of the 13th ACM Workshop on Hot Topics in Networks (HotNets-XIII). ACM, New York, NY, USA, Pages 22, 7, 2014.
20. P. Porras, S. Cheung, & M. Fong, "Securing the software-defined network control layer," in. Proc.NDSS, San Diego, CA, USA, pp.1-15, 2015.
21. P Porras, S Shin, V Yegneswaran, M Fong, M Tyson, G Gu. 2012. A security enforcement kernel for OpenFlow networks. In Proceedings of the first workshop on Hot topics in software defined networks (HotSDN '12). ACM, New York, NY, USA, pp 121-126, 2012.
22. D Kreutz, F.M.V. Ramos, P E Verissimo, E.R Christian, S. Azodolmoky, S Uhlig Software-Defined Netwoking: A Comprehensive Survey. Proceedings of The IEEE. Vol. 103, No. 1, 14-76, 2015.
23. OpenFlow Switch Specification, 1.5.1 (March 2015) URL https://www.opennetworking.org/wp-content/uploads/2014/10/openflow-switch-v1.5.1.pdf

AUTHORS PROFILE

Raktim Deb, Ph.D. Scholar in the Department of Computer Science and Engineering, Assam University, Silchar, Assam, India. He is an IEEE student member. His research interest is Software Defined Networks, Cloud Computing.

Sudipta Roy, Ph.D., is a Professor in the Department of Computer Since and Engineering, Assam University, Silchar, Assam, India. He was associated with ACE Consultant, Kolkata as a Software Professional and Bengal Institute of Technology, Kolkata, India as a faculty. His research interests are Image Processing, Software Defined Networks. He has published numerous papers in reputed journals and conference proceedings. He is an IEEE senior member and also a member of FIETE, LMCSI, MIE, MINNS, LMISTE.