International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

Framework for Access Policy for Boosting Secure Communication at SDN in FIA

Vidya M S, Mala C Patil

Abstract*: The future internet architecture is considered as a revolutionary paradigm of network owing to its capability of extensive connectivity of various forms of computing as well as communication devices. For the purpose of establishing a connection, there are various forms of protocols associated with communication defined for network and physical layer. Unfortunately, they are not benchmarked by any authorized regularity. Therefore, these forms of networks are exposed to a significantly higher level of security threats. Cross-Scripting Attack is one such rising security concern for future internet architecture that is found very less investigated in existing times. Hence, in this aspect, the software-defined network could offer a significant security solution on the top of future internet architecture. It could offer a good balance of security and reduced communication overhead as the controller can undertake a decision about the communication route that is cost-effective as well as secured. This paper highlights a discussion about a novel access control protocol that monitors and evaluates all the incoming traffic and offers an identification process for potential threats over the switching mechanism of the software-defined network. The proposed study doesn't make use of any form of conventional encryption mechanism and uses a middleware system in order to assess the severity of the attack. Upon identification, the adversaries are isolated from the targeted traffic safeguarding the network from a cross-scripting attack.

***Keywords*: Future Internet Architecture, Software Defined Network, Cloud,** **Cross-Scripting Attack**.

I. INTRODUCTION

In the past few decades, the scale of the Internet has evolved from small communication network platforms to a wide range of commercial platforms [1]. It has turned into an integral part of daily human lives as well as a noteworthy part of economic operations and social connectivity [2]. In addition, the Internet has molded striking openings to advance knowledge across the range of human accomplishments [3]. The success of the Internet has led to very high expectations and conception for future applications and advance services, in which the existing Internet may unable to abetment or lift to a satisfactory level [4].

Revised Manuscript Received on February 28, 2020.
***** Correspondence Author
Vidya M S*, Assistant Professor, Department of Computer Science & Engineering, BMSIT& M, Bangalore, India, Email: rvidyapai@bmsit.in
Mala C Patil, Assistant Professor, Department of Computer Science, COHB University of Horticultural Sciences, Bagalkot, India, Email: malapatil2002@yahoo.co.in

However, the speedy development in the networking and computing technology has introduced a new paradigm called Software-Defined Networking (SDN) [5] and has realized a variety of applications from cloud computing, smart home, industrial monitoring to healthcare services [6-10]. However, the design principles such as scalability, adaptability, and universality of the Internet have contributed to a unique trend of innovation and modernism. However, the growing demand for reliable and seamless communications by users has brought new challenges, and these challenges have given the existing Internet is under pressure that is originally intended to assist communication between end devices[11]. Internet hosting services have shown explosive growth. The nature of the future Internet is a very large-scale kind, virtualized, highly reliable, and versatile, that allows users to easily access various services with independent of any location and time. The future internet architecture-(FIA) must be adaptive to offer reliability, availability, and privacy to various service models and requirements [12-13]. In this regard, FIA requires increased robustness, survival, and collaborative qualities. Also, the built-in functions and indispensable components of the FIA architecture are one of the essential components of security [14]. There is no doubt that the most significant part of data transmission and communication is executed over the internet channel, which is vulnerable to various cyber attackers [15]. Unfortunately, regardless of the use of expensive firewall systems, existing Internet architectures lack robustness and the ability to identify and block all deadly forms of attacks. In the FIA, it is possible that some of these attacks may continue to lead in the form of their enhanced versions. The most common web-attacks are Trojans, malware, SQL injection, phishing, Denial of Service-(DoS), credential reuse, session hijacking, and many more [16-17]. Various studies have been conducted towards addressing cyber-attacks in futuristic internet eco-system. Although various types of security mechanisms have been introduced in recent years, however, existing security is insufficient to meet global security and privacy requirements [18-20]. Therefore, an effective security mechanism is needed, which can ensure strong security and privacy through a complete solution. Therefore, this paper proposes modeling of a novel access control system that can perform identification of major threats followed by isolation of it in SDN based switching system in FIA. The rest of the portions of this paper are organized as follows: Section-II presents a review of the literature. Section-III, highlights the research problem. Section-IV discusses the research methodology. Section-V presents the algorithm implementation design and its description. Section-VI presents the result and outcomes of the proposed methodology, and finally, the conclusion of the entire work is presented in Section VII.

II. RELATED WORK

Security and privacy are major issues for users who exist in web-based networking and communication eco-system. Various research efforts have been proposed in the literature to ensure network security towards allowing multiple devices and users to participate in a reliable and secure environment. The work carried out by Alshra et al. [21] introduced, security approach based on the implementation of the isolated hardware device with the SDN system to prevent controller component from a packet injection attack. Another work done by Abdullaziz et al. [22] presented a lightweight authentication scheme using the bitwise operation to secure the SDN controller against a DoS attack. Here, a bitwise operation is used to hide the Ids of the transmitting nodes into the control packets. The work of Eom et al. [23] suggested a conceptual security framework where the authors have carried threat modeling and performed SDN security evaluation considering multiple parameters such as network centrality measure, attack impact score, and vulnerability score. Rasool et al. [24] exposed the security risk associated with SDN and its vulnerability to link flooding attacks. The author in this study then introduces a different countermeasure model designed using deep learning techniques for classifying network traffic to mitigate LFA in SDN. Sallam et al. [25] explored the challenges and issues associated with the SDN network and presented a security model using the client gateway SDP framework. The authors in the study of Varadharajan et al. [26] introduced a rule-oriented security model for distributed SDN that enables inter and intra domain secure communications processes between different hosts. This approach is useful in securing sensitive data and meets specific routing and path security requirements compared to the traditional method. A security plan for protecting the control plane against Distributed DoS attacks is presented in the study of Wang et al. [27]. The presented scheme is formulated into two modules i.e., abnormal traffic identification and defensive mechanism. The important quality of this approach is the deployment of multiple controllers in the control plane through a cluster of controllers. Yang et al. [28] suggested a method designed based on the joint approach of anomaly identification and a multi-layer response model. Anomaly identification checks for abnormal behavior from the state of the physical process and a multi-layer response model prevent unauthorized packet communication, thereby generating a strategy to mitigate attacks to protect the physical process. Geng et al. [29] have suggested dual security strategies for vehicle network. Initially, the network hierarchy was composed of software-defined concept to normalize the network management. Based on this fact, various security protocols are embedded to prevent common security attacks in the network. Meng et al. [30] concentrated on detecting insider attacks in clinical SDN. Here, the author first conducted an investigation and designed a trust-based method using Bayesian inference to find malicious devices in a medical environment. Wang et al. [31] presented a security mechanism to resist DoS attacks in the SDN controller. The presented security mechanism mainly includes multiple implementation modules such as DoS detection module, forecasting engine module, priority manager module, and the last one is the scheduler module. The performance of the presented approach is assessed in terms of OpenFlow environments.

The study outcome demonstrates that the presented approach is efficient for ensuring robust security with limited overhead. Achleitner et al. [32] defined a strategic method to prevent network services against network reconnaissance and designed a reconnaissance deception system. The main purpose of this method is to cancel information of the attacker, and delayed the operation of finding vulnerable hosts, and determined the source point of attacks in the network.

In the study of Xu et al. [33], a review work is performed to examine the impact of the table-overflow attack on the SDN. The authors found that the existing solutions are not much suitable to defend such kinds of attacks in the SDN-oriented network system. In order to overcome the limitation of existing solutions, the study has presented an attack detection mechanism based on traffic features and mitigation mechanisms using a token bucket scheme.

Yan et al. [34] suggested a scheduling approach using a time-slice allocation mechanism to ensure the availability of SDN services under a distributed-DoS attack. Similarly, the work of Yoon et al. [35], have also carried a comprehensive study towards attacks in SDN OpenFlow network. Here, the author discusses the taxonomy to gain understanding into general pitfalls that make SDN stacks corrupted under hostile computing environments. The work of Deng et al. [36] revealed a different form of vulnerability associated with SDN and introduced a packet injection attack than creating a bad impact on the network topology management and rest API, on the SDN controller.

The authors then designed a lightweight mechanism of the packet-catcher existing SDN controller to mitigate the impact of this attack. Lal et al. [37] suggested a hybrid scheme that includes physical layer security, SDN, node collaboration, context awareness, and cross-layer.

The suggested scheme implements at both nodes level and network-level those are compatible with network conditions, and possible attacks. Cui et al. [38] collected data from hosts positioned globally using a realistic SDN network to understand the SDN network fingerprints of remote adversaries.

The authors analyzed that using Round trip time information and data packet exchange information, the probability of fingerprint attacks on SDN networks is very high. Lara and Ramamurthy [39] introduced a policy-based security mechanism that allows network operators to describe security policies using easy-to-understand scripts and enforce these policies in the network to implement automatic responses to security and provide Security operators hide the complexity of the network. The work carried out by Luo et al. [40] a multi-stage attack mitigation scheme for the smart home application using SDN and Network Function Virtualization to mitigate multi-layer attacks.

III. RESEARCH PROBLEM

There are various literatures to claim that Content-Centric Network-(CNN) is an integral part of FIA, but there is no discussion of an implementation to boost up the data security. Existing researchers working on cloud security has dominantly used public key encryption without assessing their computational complexity as well as response time. It is quite evident that public key encryption will consume more resources as well as computational processing time if they are allowed to work on highly distributed environment irrespective of their claimed reliable security. At the same time, existing key management techniques over cloud computing as hosting existing internet architecture doesn't offer full fledge secret key security. It cannot ensure both forward and backward security at same time during algorithm implementation. In this entire scenario of implementation, it can be seen that data, which is primarily content in Content-Centric Network is never safe when allowed to be transmitted in highly distributed channels in FIA. Dependencies over third party application do exists today but in such cases the ownership of the data as well as privacy information of the data (or content) owner is at greater risk. Therefore, there is a need to design a fail-proof access control system that is capable of identifying the legitimate user over cloud and permit them access without involving much complicated steps of authentication. At the same time, the user's private data as well as owned content are required to be kept on top priority while performing secure communication over applications running on FIA. The following are significant research gap analyzed after a closer analysis of into existing web security and existing FIA projects.

- It has been analyzed that there are more research attempts for web security than FIA security. However, research on network security has not considered the FIA standard and vice versa.
- Most existing security mechanism for FIA are designed considering specific attacks like Pollution attacks, table overflow attacks, suppression attacks, collusion attacks, etc. Little research has focused on cross-site scripting.
- FIA is considered sanitary communication framework built on multiple components. However, no FIA-related projects (e.g. NEBULA, MobilityFirst, etc.) have emphasized the trend to develop robust components for enabling robust FIA.
- SDN provides proper network management for IoT operations in FIA; however it is vulnerable to many kinds of security threats and attacks. The existing interface design of SDN is not subjected to completely safe and secure to control its controller system thereby resulting results in inadequate access control system.

The next section presents a novel security mechanism to accomplish its objective of achieving unique access control system recognize fatal threats linked with cross scripting attack over FIA.

IV. RESEARCH METHODOLOGY

This part of the study is a continuation of our prior work [41-43]. The prime aim of the proposed study is to develop a mechanism of a distinct access control in order to identify lethal threats associated with cross scripting attack over future internet architecture. This part of the study implementation is meant for further improving the access control policies for addressing the security pitfalls of SDN when used for switching communication in FIA. The study also targets to identify the normal traffic to malicious traffic and assists in isolating the adversaries to intrude the SDN based switch operation.

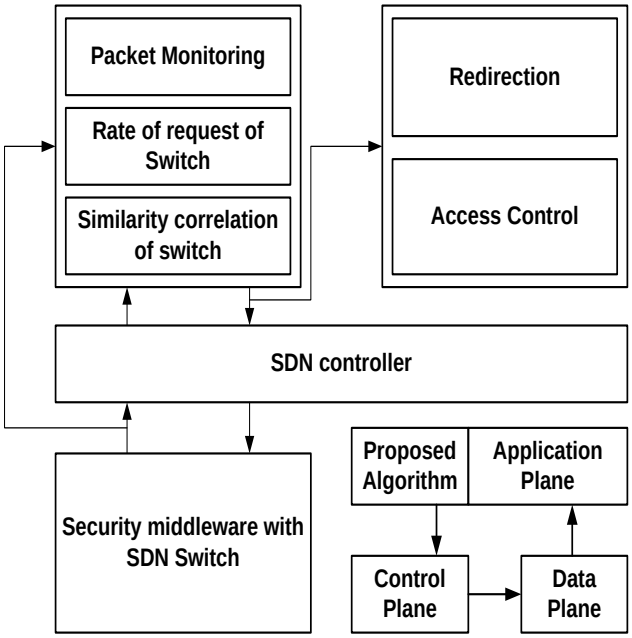

Fig.1. Proposed Research Methodology

A mathematical modeling will be adopted in this part of research methodology for constructing a novel and cost effective secure access control policy in SDN based switching operation in FIA. Fig.1 highlights the methodology to be adopted for this purpose. One of the essential contributions of the proposed implementation planning is not to use any form of cryptographic policy for designing access control policy. A mathematical model will be constructed that allows forwarding of all the unusual request to the control plane of SDN unlike the existing approach where the request is directly subjected to routing rules of SDN. An algorithm will be constructed to check if the data packet has any form of correlation with existing or prior traffic flows in its cache. A new format of beacons will be constructed for this purpose that record IP address and payload information of the switch and message. This process will assists in differentiating the normal flow from abnormal (or malicious) flow in SDN based switches in FIA. The next part of implementation will be to offer resistance once malicious message is identified and recorded on the control link. The resistance is offered by allocating control access dynamically. The proposed system will enable the SDN switch to perform routing operation, identifying of threats, and allocation of dynamic policies to access network.

Based on this input, the control plane will choose to either forward the incoming request or drop the incoming request over distributed network. Basically, the idea is to ensure that invoking of non-encryption approach towards the switching mechanism should further strengthen the security of the software defined network.

V. ALGORITHM IMPLEMENTATION

The proposed system implements an algorithm that offers added security advantage to the software defined network towards protecting future internet architecture. The idea is mainly to resist adversarial effect of cross-site scripting without using any form of conventional algorithm. The algorithm is constructed for this purpose whose essential steps of operation are as shown below:

Algorithm for Secure Route Construction

Input: P_{sw} (prime switch), E_{sw} (Edge Switch), S (Servers)

Output: r (routes)

Start

1. *init* P_{sw}, E_{sw}, S, c_{capd}, c_{cap}
2. d_{entry} =[$Prof_{ID}$, CSLoC, UT,CS]
3. generate jobs(Psw, Esw, S, u)
4. **For** i=i: S
5. **For** j=1: c_{cap}
6. **For** k=1: size(d_{entry})
7. obtain zone of current request
8. compare each zone
9. **For** l=1:S_{rem}
10. N=N(l)+1;
11. **End**
12. N=N(rix)
13. Compute Ms→V_{cap} / V_{slice}
14. **End**
15. **End**
16. **End**
17. apply *f*(x)=r

End

The complete algorithm is executed over various steps. In the first step, the algorithm takes the necessary input for modeling user request that consists of profile identity $Prof_{ID}$, content server location CSLoC, upload time UT, content size CS (Line-2). All this information is retained in a matrix d_{entry} (Line-2) while other related software defined network variables of switching are also initialized e.g. prime switch P_{sw}, edge switch E_{sw}, number of servers *S* (Line-1). The next part of the algorithm is to generate jobs so that communication can be initiated in the future internet architecture. For this purpose, the algorithm has to consider demands of channel capacity c_{capd}, which is initiated, along with other variables. The jobs are generated on the basis of matrix dentry and random allocation of c_{capd}. The consecutive evaluation is carried out considering all the servers S (Line-4), channel capacity c_{cap} (Line-5), and all the rows of the matrix d_{entry} (Line-6). The algorithm computes the ranges of the traffic in each communication area followed by computation of request number over each communication area. All the communication regions are compared logically with the elements of the d_{entry} matrix (Line-7 and Line-8). The next part of the algorithm implementation is about considering all the remaining servers S_{rem} (Line-9) and look for quantity of the server in each communication area. This computation (Line-10) is carried out considering the reduced number of virtual machine at each communication area. All the servers located at each communication area are then randomized where the variable rix represent a matrix holding all the random servers over each communication region (Line-12). The algorithm initializes capacity (V_{cap}) as well as slices of virtual machine (V_{slice}) in order to obtain the memory occupied per slice (Ms) as shown in Line-13. The algorithm considers all the users of software defined network where the respective request of traffic and current request are obtained. The communication area are connected with server as well as the request while all the respective server in the communication area are arbitrarily connected. The interesting point here is that there is no pattern and hence attacker will never able to find out the source point if they are monitoring the traffic. Larger the number of nodes, larger is the randomness and more is security towards accessing the network. The system also computes the usage of slices and indexes them respectively that it has been already read followed by computation of slice number demanded. It is computed by updated matrix of d_{entry} divided by Ms. However, if the number of slices are found not to be sufficient than it is taken from other server located in same communication region. However, if the available slot is witnessed with less memory than demanded slice is considered from different zone. Adoption of this strategy ensure that the algorithm doesn't run short of resources when they are in process of monitoring or resisting intrusions in future internet architecture. This operation is a novel contribution and excels better than encryption approach. While usage of encryption approach drains the resources of single entity, but proposed approach ensures that resources in budget is sufficient enough to deal with communication need; however, if any extra resources are demanded, it can be obtained from next neighboring communication area. The proposed system performs this routing approach in highly flexible manner.

The final part of the algorithm is to construct a function *f*(x) and apply on proposed system for performing secured data transmission. The operation of this function are basically based on two significant tracking attributes viz. the rate of request from switch as well as the similarity correlation of the switches. The rate of request for the switch of software defined network depicts the quantity of different packets that are assessed during test instance. This is extremely important attribute for both the malicious traffic as well as normal traffic. It should be also known that the similarity correlation of the switch is actually a depiction of mean rate of traffic entries (d_{entry}) at that particular time instance. This operation is constructed in order to distinguish malicious traffic and regular traffic. Once the redirection command is given by the algorithm for routing, all the non-similar data packets (irrespective of their intention of safer or attack) are forwarded to the middleware system of software defined network.

Hence, the maliciously injected data cannot launch consecutive malwares of cross scripting either in control plane or in data plane. The chances of further getting compromization is less as middleware are generally much secured and they offers potential resistivity from malicious traffic. Therefore, the security feature of software defined network is significantly improved in dual fold viz. i) secured routing and ii) lower resource consumption towards resisting cross-scripting attack.

VI. RESULT

This section discusses results obtained after carrying out the simulation study in MATLAB. The analysis is carried out considering both communication factor and security factor for proving how it can identify and resist cross scripting attack over future internet architecture.

A. Analysis Strategy

In order to form an artificial environment of cross scripting attack, the proposed system artificially injects malicious script into the traffic flow. The idea is to find the presence of such intention while performing communication over switching system in software defined network. The monitoring is carried out to check if identification performances as well as communication performance over the switches are well maintained.

B. Communication Performance Analysis

The proposed system is compared with the existing encryption approach used for resisting cross-scripting attack in future internet architecture. Various encryption approaches e.g. SHA-1, SHA-2, AES are applied and outcomes are averaged in order to compare with the proposed system with respect to packet delivery ratio and channel capacity.

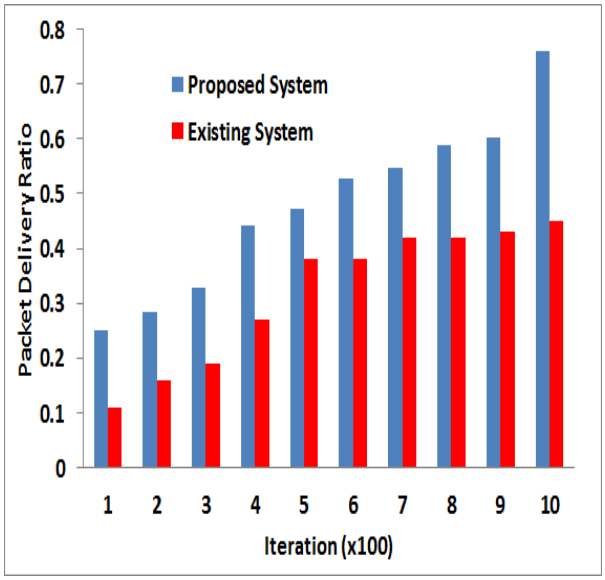

Fig.2. Comparative Analysis of Packet Delivery Ratio

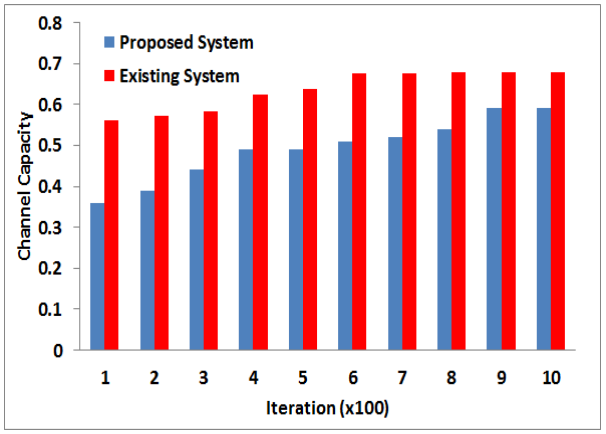

Fig.3. Comparative Analysis of Channel Capacity

Fig.2 and Fig.3 highlights that proposed system offers better packet delivery ratio as well as reduced dependencies of channel capacity. Increased in packet delivery ratio shows that proposed system withholds all the malicious traffic. As the identification is carried out in middleware, so processing of incoming traffic doesn't gets affected resulting in better delivery performance. The proposed system also offers better flexibility over adding additional servers to further process jobs results in significant control of channel capacity, which usually shoots up during the cross-scripting attack.

C. Attack Mitigation Performance Analysis

The percentage of attack mitigation is evaluated by computing number of confirmed identified attack and number of suspicious traffic that has been isolated. The outcome in Fig.4 shows that proposed system has significantly better identification rate compared to existing algorithms of security. The prime reason behind this performance is that proposed system makes use of packet monitoring approach using cost effective routing strategy. Hence, more information is relayed by the nodes in software defined network where the controller can undertake appropriate decision for resisting the malicious routes infected by the cross scripting attack. Unfortunately, existing encryption approach is iterative and not-flexible which fails them to identify the attack routes.

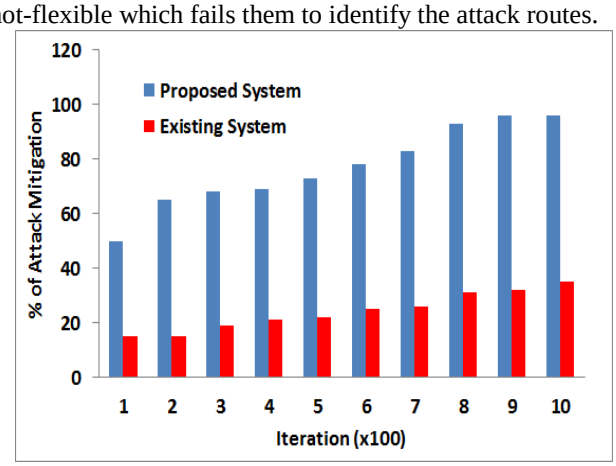

Fig.4. Percentage of Attack Mitigation

D. Computational Performance Analysis

From the computational performance, the proposed system is evaluated with respect to algorithm processing time. Fig.5 shows that proposed system offers significantly less consumption of algorithm processing time in contrast to existing system.

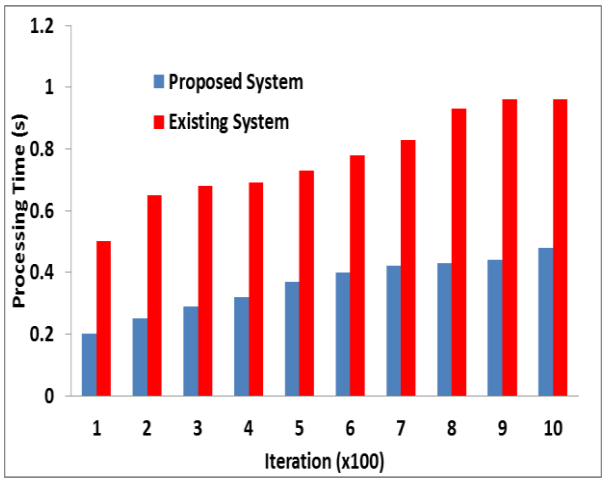

Fig.5. Comparative Analysis of Processing Time

The prime reason behind this is that proposed system is completely non-iterative and immensely progressive in its order of implementation. This results in much lesser time consumption which is not the case with existing encryption algorithms that are highly recursive in their operation. This proves that proposed system is highly compatible with the distributed system which executes over software defined network.

From the above result analysis, it can be realized that proposed system without using any form of sophisticated principles offers better results from both security and communication viewpoint.

VII. CONCLUSION

This proposed system introduces a mechanism that offers solution towards safeguarding breaches in software defined network especially in control and data plane. The attack considered for analysis is cross-scripting attack which is found mainly over injected packets in massive traffic scenario.

This leads to truncation of communication between the user devices and servers in future internet architecture. Depending upon the type of approaches in existing system, the proposed system, the proposed system is classified to perform both identification of cross scripting attack and isolating it. The proposed system constructs a novel access control policy that exploits the routing information and manages the transacted messages between the controller system and switching system of software defined network.

The idea was also to offer cost effective security solution such that communication performance and security performance is well balanced. The study outcome shows that proposed system offers better cumulative performance in comparison to frequently used encryption policies over software defined network in case of future internet architecture.

REFERENCES

1. B. Yang, Y. Lu, K. Zhu, Y. Zhang and J. Liu, "Evolution of the Internet and its measures," 2017 First International Conference on Electronics Instrumentation & Information Systems (EIIS), Harbin, 2017, pp. 1-4.
2. Yang, Dan, and Zhihai Rong. "Evolution of the internet at the autonomous system level." In 2015 34th Chinese Control Conference (CCC), pp. 1313-1317. IEEE, 2015.
3. Acharjya, D. P., M. Kalaiselvi Geetha, and Sugata Sanyal, eds. Internet of Things: novel advances and envisioned applications. Vol. 25. Heidelberg: Springer, 2017.
4. Jain, Raj. (2006). Internet 3.0: Ten Problems with Current Internet Architecture and Solutions for the Next Generation. 1-9. 10.1109/MILCOM.2006.301995.
5. Gong, Yili, Wei Huang, Wenjie Wang, and Yingchun Lei. "A survey on software defined networking and its applications." Frontiers of Computer Science 9, no. 6 (2015): 827-845.
6. Bera, Samaresh, Sudip Misra, and Athanasios V. Vasilakos. "Software-defined networking for internet of things: A survey." IEEE Internet of Things Journal 4, no. 6 (2017): 1994-2008.
7. Chang, Kai-Di, Chi-Yuan Chen, Jiann-Liang Chen, and Han-Chieh Chao. "Internet of things and cloud computing for future internet." In International Conference on Security-Enriched Urban Computing and Smart Grid, pp. 1-10. Springer, Berlin, Heidelberg, 2011.
8. Radhika, C., and M. Menaka. "Survey on IoT Technologies for Home Automation System." International Journal of Engineering and Techniques 2, no. 6 (2016): 159-165.
9. Jaloudi, Samer. "Communication Protocols of an Industrial Internet of Things Environment: A Comparative Study." Future Internet 11, no. 3 (2019): 66.
10. Mayora, O., Sucar, L.E. Editorial: Applications of Future Internet. Mobile Netw Appl 24, 1639–1640 (2019) doi:10.1007/s11036-019-01230-w
11. Sathiaseelan, Arjuna, Dirk Trossen, Ioannis Komnios, Joerg Ott, and Jon Crowcroft. "An internet architecture for the challenged." In IAB ITAT Workshop. 2013.
12. Shenker, Scott. "Fundamental design issues for the future Internet." IEEE Journal on selected areas in communications 13, no. 7 (1995): 1176-1188.
13. Correia, Luis M., Henrik Abramowicz, Martin Johnsson, and Klaus Wünstel, eds. Architecture and design for the future internet: 4WARD project. Springer Science & Business Media, 2011.
14. Papadimitriou D. et al. (2012) Design Principles for the Future Internet Architecture. In: Álvarez F. et al. (eds) The Future Internet. FIA 2012. Lecture Notes in Computer Science, vol 7281. Springer, Berlin, Heidelberg
15. Liu Y., Wang Z., Tian S. (2019) Security Against Network Attacks on Web Application System. In: Yun X. et al. (eds) Cyber Security. CNCERT 2018. Communications in Computer and Information Science, vol 970. Springer, Singapore
16. Jang-Jaccard, Julian, and Surya Nepal. "A survey of emerging threats in cybersecurity." Journal of Computer and System Sciences 80, no. 5 (2014): 973-993.
17. Awang N.F., Manaf A.A., Zainudin W.S. (2014) A Survey on Conducting Vulnerability Assessment in Web-Based Application. In: Hassanien A.E., Tolba M.F., Taher Azar A. (eds) Advanced Machine Learning Technologies and Applications. AMLTA 2014. Communications in Computer and Information Science, vol 488. Springer, Cham
18. Babiker, Mohammed & Karaarslan, Enis & hoscan, yasar. (2018). Web Application Attack Detection and Forensics: A Survey. 10.1109/ISDFS.2018.8355378.
19. Chaabouni, Nadia, Mohamed Mosbah, Akka Zemmari, Cyrille Sauvignac, and Parvez Faruki. "Network Intrusion Detection for IoT Security based on Learning Techniques." IEEE Communications Surveys & Tutorials (2019).
20. Chowdhury, Abdullahi. (2016). Recent Cyber Security Attacks and Their Mitigation Approaches ? An Overview. 54-65. 10.1007/978-981-10-2741-3_5.
21. A. S. Alshra'a and J. Seitz, "Using INSPECTOR Device to Stop Packet Injection Attack in SDN," in IEEE Communications Letters, vol. 23, no. 7, pp. 1174-1177, July 2019.

22. O. I. Abdullaziz, L. Wang and Y. Chen, "HiAuth: Hidden Authentication for Protecting Software Defined Networks," in IEEE Transactions on Network and Service Management, vol. 16, no. 2, pp. 618-631, June 2019.
23. T. Eom, J. B. Hong, S. An, J. S. Park and D. S. Kim, "A Systematic Approach to Threat Modeling and Security Analysis for Software Defined Networking," in IEEE Access, vol. 7, pp. 137432-137445, 2019.
24. R. U. Rasool, U. Ashraf, K. Ahmed, H. Wang, W. Rafique and Z. Anwar, "Cyberpulse: A Machine Learning Based Link Flooding Attack Mitigation System for Software Defined Networks," in IEEE Access, vol. 7, pp. 34885-34899, 2019.
25. [25] A. Sallam, A. Refaey and A. Shami, "On the Security of SDN: A Completed Secure and Scalable Framework Using the Software-Defined Perimeter," in IEEE Access, vol. 7, pp. 146577-146587, 2019.
26. V. Varadharajan, K. Karmakar, U. Tupakula and M. Hitchens, "A Policy-Based Security Architecture for Software-Defined Networks," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 4, pp. 897-912, April 2019.
27. Y. Wang, T. Hu, G. Tang, J. Xie and J. Lu, "SGS: Safe-Guard Scheme for Protecting Control Plane Against DDoS Attacks in Software-Defined Networking," in IEEE Access, vol. 7, pp. 34699-34710, 2019.
28. J. Yang, C. Zhou, Y. Tian and S. Yang, "A Software-Defined Security Approach for Securing Field Zones in Industrial Control Systems," in IEEE Access, vol. 7, pp. 87002-87016, 2019.
29. R. Geng, X. Wang and J. Liu, "A Software Defined Networking-Oriented Security Scheme for Vehicle Networks," in IEEE Access, vol. 6, pp. 58195-58203, 2018.
30. W. Meng, K. R. Choo, S. Furnell, A. V. Vasilakos and C. W. Probst, "Towards Bayesian-Based Trust Management for Insider Attacks in Healthcare Software-Defined Networks," in IEEE Transactions on Network and Service Management, vol. 15, no. 2, pp. 761-773, June 2018.
31. T. Wang, Z. Guo, H. Chen and W. Liu, "BWManager: Mitigating Denial of Service Attacks in Software-Defined Networks Through Bandwidth Prediction," in IEEE Transactions on Network and Service Management, vol. 15, no. 4, pp. 1235-1248, Dec. 2018.
32. S. Achleitner, T. F. La Porta, P. McDaniel, S. Sugrim, S. V. Krishnamurthy and R. Chadha, "Deceiving Network Reconnaissance Using SDN-Based Virtual Topologies," in IEEE Transactions on Network and Service Management, vol. 14, no. 4, pp. 1098-1112, Dec. 2017.
33. T. Xu, D. Gao, P. Dong, C. H. Foh and H. Zhang, "Mitigating the Table-Overflow Attack in Software-Defined Networking," in IEEE Transactions on Network and Service Management, vol. 14, no. 4, pp. 1086-1097, Dec. 2017.
34. Q. Yan, Q. Gong and F. R. Yu, "Effective software-defined networking controller scheduling method to mitigate DDoS attacks," in Electronics Letters, vol. 53, no. 7, pp. 469-471, 30 3 2017.
35. C. Yoon et al., "Flow Wars: Systemizing the Attack Surface and Defenses in Software-Defined Networks," in IEEE/ACM Transactions on Networking, vol. 25, no. 6, pp. 3514-3530, Dec. 2017.
36. S. Deng, X. Gao, Z. Lu and X. Gao, "Packet Injection Attack and Its Defense in Software-Defined Networks," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 3, pp. 695-705, March 2018.
37. C. Lal, R. Petroccia, K. Pelekanakis, M. Conti and J. Alves, "Toward the Development of Secure Underwater Acoustic Networks," in IEEE Journal of Oceanic Engineering, vol. 42, no. 4, pp. 1075-1087, Oct. 2017.
38. H. Cui, G. O. Karame, F. Klaedtke and R. Bifulco, "On the Fingerprinting of Software-Defined Networks," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 10, pp. 2160-2173, Oct. 2016.
39. A. Lara and B. Ramamurthy, "OpenSec: Policy-Based Security Using Software-Defined Networking," in IEEE Transactions on Network and Service Management, vol. 13, no. 1, pp. 30-42, March 2016. [40] S. Luo, J. Wu, J. Li and L. Guo, "A multi-stage attack mitigation mechanism for software-defined home networks," in IEEE Transactions on Consumer Electronics, vol. 62, no. 2, pp. 200-207, May 2016.
40. Vidya, M. S., and Mala C. Patil. "Qualitative Study of Security Resiliency Towards Threats in Future Internet Architecture." In Proceedings of the Computational Methods in Systems and Software, pp. 274-284. Springer, Cham, 2018.
41. Vidya, M. S., and M. C. Patil. "Reviewing effectivity in security approaches towards strengthening internet architecture." Int. J. Electr. Comput. Eng.(IJECE) 9, no. 5 (2019): 3862-3871.
42. Vidya, M. S., and Mala C. Patil. "A Novel Schema for Secure Data Communication over Content-Centric Network in Future Internet Architecture." In Proceedings of the Computational Methods in Systems and Software, pp. 256-265. Springer, Cham, 2019.

AUTHORS PROFILE

Vidya M S, completed B.E from Gulbarga University, M. Tech from VTU and pursuing PhD under VTU. Her area of Research is Network Security, and has teaching experience of 14 years. Published papers in National and International journals.

Dr Mala C Patil, working as an assistant professor, department of computer science, COHB University of Horticultural Sciences, Bagalkot, India, She has completed her PhD from Anna University. She has done B.E from Karnataka University, Dharwad, M.S from bits Pilani. She has teaching experience of 25 years. Her area of research is Software Engineering. She has Published papers in various national and international journals.