ISSN No:-2456-2165

A Survey of Intrusion Detection Techniques on Software Defined Networking (SDN)

Ahmad Ajiya Ahmad[1], Prof. Souley Boukari[2], Abdullahi Musa Bello[1], Mustapha Aliyu Muhammad[2]
[1]Department of Computer Science, Faculty of Science, Federal University Gashua, Yobe State, Nigeria
[2]Mathematical Science Department, Abubakar Tafawa Balewa University, Bauchi Sate, Nigeria

Abstract:- Software Defined Network (SDN) is a network model in which traffic may be controlled and managed robustly while ensuring that the system is protected from potential attacks in accordance with client requests. SDN is an emerging technology that is presented with the purpose to reduce the complexity of network functioning by splitting the data and control layer. However, the splitting contributes to a security challenge which is one of the enormous issues concerning SDN operation. Several attack classes such as Distributed Denial of Service (DDoS) attacks may befuddle the SDN performance as a result of the separation. Recently, different methods have been developed in the SDN-based Network Intrusion Detection Systems (NIDS) in order to safeguard computer systems and to overcome SDN security challenges. Besides, various current literature on intrusion detection techniques which influence SDN networks has been reviewed and analyzed in this paper. These Intrusion detection techniques are implemented and help to triumph over SDN network security problems.

Keywords:- *Software Defined Network, Data Layer, Control Layer, Distributed Denial-of-Service, Network Intrusion Detection Systems.*

I. INTRODUCTION

The traditional or legacy networks have grown exponentially such that it becomes a problem to handle malicious activities in the network because of the scalability of the network [10]. These Cyber-attacks have developed a threat to recognized industries and enterprises. Malicious attacks eliminate, steal, damage, modify and gain access to essential sensitive data. SDN is a novel technology widely used that is manageable, dynamic, economical ease, and flexible, making it perfect for the improved security, performance, and dynamic nature of today's systems [29]. The main idea behind the SDN development is the separation of data and control layer. That is the architecture of SDN is detached into three layers, application layer, control layer, and data layer. On contrary, the traditional network solution combines both the data and control layer together. SDN architecture offers numerous advantages compared to the traditional network [23]. The Application layer comprises diverse applications essential for numerous business necessities. These applications are software programs which implemented on the SDN control layer on the centralized controller. SDN applications interconnect with the controller by a northbound interface in accordance with their network requests. The Control layer implemented all the control logic of the system and comprises a single or multiple controllers that act as the main "brain" of SDN that controls the entire network switches and manages the whole network functionalities by comprehensive monitoring and management of the network [17]. The data layer comprises of network devices such as switches and routers responsible to forward all the packets on the network [31]. These devices are interconnected with one another through a wired or wireless medium. Figure 1 shows the comprehensive SDN architecture with the indication of different layers.

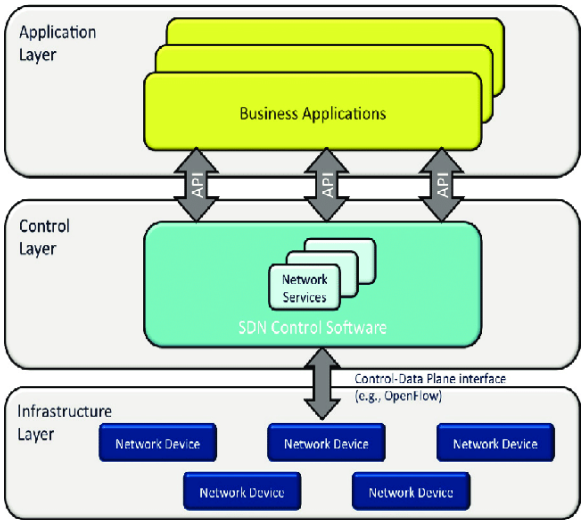

Fig 1. Software Defined Networking (SDN) Architecture

Unfortunately, the implementation of the SDN architecture could result in numerous kinds of problems to the SDN controller and OpenFlow networks, such as an attack, vulnerabilities, and threat vectors [5]. SDN security has to turn out to be an exceptional subject for academic researchers in the modern era and SDN has been supported to alleviate intrusion attacks in cyberspace. Equally, an attacker may effectively convey out an attack on the SDN network itself [20]. Therefore there is a need to solve the security challenges by Introducing Network Intrusion Detection System (NIDS) in order to detect intrusion attacks. This article aims to specify and identify the strengths and weaknesses of various research works on SDN-based network intrusion detection systems. Furthermore, the prediction of attacks classes and intrusion detection techniques involved in an SDN network will also be identified.

ISSN No:-2456-2165

II. OVERVIEW OF INTRUSION DETECTION SYSTEMS

A. Intrusion Detection System

As cyberspace increases nowadays, the number of intrusion activities every day raises globally [31]. In view of that, cyber-attacks needs to be controlled accordingly in order to stop unauthorized activities and protect sensitive information. Three important concepts of information security needs to be considered and protected in the cyberspace against the intruder. These concepts are integrity, confidentiality and availability [32].

Additionally, The split-up and centralized view of the SDN network architecture of the forwarding (infrastructure) layer and the control layer produces a novel prospect for the intruders to convey out various classes of attacks. The kinds of attacks are different compared to attacks that usually affect the traditional network [35]. For instance, the attacker can produce a new attack on the SDN controller or even the communication route between the SDN controller and OpenFlow switches. Moreover, compromised operators can be engaged to develop a fresh attack after the traffic flow is generated. As well, SDN applications can have numerous vulnerabilities that can generate attack prospects and assist intruders to bypass authentication methods and have access to the controller by mounting malicious scripts [29]. This will allow the attacker to lunch new attacks such as, launching DoS attack, and flow rules mishandling on the traffic packets. Cyber-attack is any kind of attacks that exploit the targets computer information systems, infrastructures, computer networks or personal computer devices, using different techniques in order to modify, damage, snip, data or information systems [8]. There are different classes of attacks commonly in the cyberspace such as, Distributed Denial-of-Service (DDoS) attacks, Probe Attacks, Man-in-the-Middle Attack, SQL Injection Attacks etc.

Intrusion detection is the process of observing and inspecting network traffic flow and system activities to identify malicious or unauthorized events [34]. Every single system application or device whose aim is to perform intrusion detection is so-called as an Intrusion Detection System (IDS). IDS are mainly deployed to protect a network against being affected by a malicious attack. There are, usually, two classes of intrusion detection scheme based on detection methods, namely signature-based detection and anomaly-based detection [23]. In signature-based detection, novel dataset is equalled with a signature database of identified and revealed attacks. Contrary, in anomaly-based detection, novel dataset is compared in contrast to a model of normal and malicious [18]. Subsequently, fresh and unidentified attacks can be identified effectively in an anomaly-based model.

There are different kinds of security tools or security defence mechanisms that are designed purposely to safeguard systems inside a cyberspace. These tools are different from each other in terms security functionality [22]. For example, firewalls are used to examine packet headers to screen outgoing and incoming traffic flow based on pre-set rules and packet header features such as, port number, IP address and protocol [12]. Firewalls generally work on the outside of network for cyber-attack protection in order to halt them before they go into the secured network [14]. Contrary, IDSs are capable to monitor events inside the secured network and not just at its outside. More so, they cannot handle command to completely stop suspicious activities and hence, require an administrator to handle their alerts [25]. Unlike IPSs, it works as IDS but are capable to proactively stop a detected threat. Figure 2 represents the overview of intrusion detection system together with its types and defence mechanism associated with it.

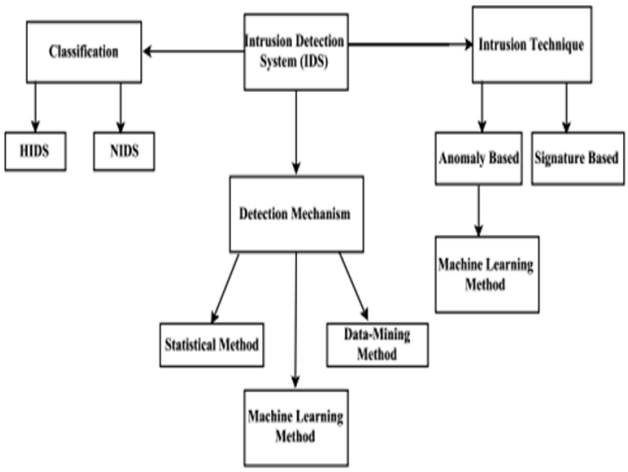

Fig 2. Types of Intrusion Detection System

B. Types of IDSs

IDSs types are classified in respect to the nature of activities that are analysed and detection method they applied. There are two types of IDSs classifies based on the nature of activities that are analysed, namely: Host-based Intrusion Detection Systems (HIDS) and Network-based Intrusion Detection Systems (NIDS). Similarly, types of IDSs classified based on detection methods applied, these are: Signature-Based intrusion detection systems and Anomaly Based intrusion detection systems.

1) Types of IDSs by analysed activities

a) Host-based IDS

Host-based Intrusion Detection Systems (HIDSs) are agents that works on data collected from individual host systems [15]. They are installed on computer systems to examine their events, such as processes, system logs, files, etc. According to [11] HIDSs could be installed to spy on the individual host by observing their activities and at the same time matched the records to check for the existence of unauthorized or suspicious activity. Even though, the major problem is, monitoring the individual system is analytical, accessibility is narrow to a particular host and the IDS process consumes resources, perhaps affecting the performance on the individual system and intrusions will not be visible or noticeable until they have already reached the individual system [38].

b) Network-based IDS

A network-based intrusion detection system generally uses smart passive devices, such as sensors, at several points on the network. These points could be at the router or host-level [29]. The passive devices do not affect the traffic flow they monitor and the exploration, scanning and detection of intrusive attacks is on a network. NIDS typically need unrestrained network access in order to analyses all traffic flows across the network [43]. NIDSs are more scalable and cross-platform, which made it widespread and is applicable for large network infrastructure to protect a company's IT equipment. NIDS solution is effective and efficient to engage concurrently to ensure a polished level of security in SDN network.

2) Types of IDSs by detection method

a) Signature Based IDS

This type of IDS possess a database generally identifies as attack signatures that contain attribute and features of known malicious threat [43]. It monitors traffic flow with the signature database and checks the input stream for the occurrence of intrusive attacks. Considering this type of IDS to be effective and efficient, the attack signatures must be updated frequently. Though, even with the newest updates, only identified attacks can be discovered using this type of IDS [45].

b) Anomaly Based IDS

Anomaly detection attempts to study a "normal or expected" activity of the system and identify kind of bandwidth, protocols and ports generally used [42]. Any aberration from this behaviour is reflected as a possible intrusion and will make an alarm. This type of IDS does not necessitate updates or existence of a database [16]. It can recognize unidentified intrusions but also generate a lot of false positives that are challenging to process. It is similarly tougher to gather evidence about the intrusion since it is not obviously recognised by a signature.

C. *Defense Mechanisms for SDN*

SDN has fascinated the attention of academics scholars globally due to its effective features for resolving and providing novel security mechanisms [30]. With the current advancement of SDN, it has been a valuable stage for the security viewpoint in the legacy networks. The universal outlook and programmability are the key structures to regulate the influence of cyber-attacks [37]. Defense mechanisms are categorized into statistical based and machine-learning (ML) based.

A statistical analysis comprises gathering and exploring the records collected to detect malicious traffic. The exploration is articulated on the foundation of the behaviour and properties of the traffic packets flow [37]. Statistical interpretation assessment is applied on the network traffic obtained, and if the records cannot be trim on certain statistical models, at that juncture they are categorized as malicious data. According to [19] Statistical/Policy based Defense Mechanisms Relies on the administrator defined policies to detect and mitigate attacks. Machine Learning has gained attention as an auspicious technique and consists of several algorithms that have been implemented for security objectives and necessities. They are also being adapted to Identify and alleviate the intrusion in SDN network [29]. These algorithms are operated as a classifier to categorize data traffic into normal and malicious. The summary of different papers on Machine Learning based detection mechanisms are enumerated in Table 1.

The machine learning algorithms can be characterized into supervised, unsupervised learning and semi supervised learning based on how they are trained. Different machine learning algorithms can be applied to identify and mitigate intrusion attacks across SDN network and the most frequently adapted algorithms are k-means clustering, neural network, naive bayes, support vector machine (SVM), genetic algorithm and self-organizing map (SOM) and fuzzy logic [37]. Machine learning is gaining victory progressively these days and are been applied positively in most of the field of computer science such as, intrusion detection, face detection, speech recognition and image processing [39].

The model of a neural network is a type of model that can be trained in both supervised and unsupervised. Almost models have supervised training and their engaged dataset comprises both inputs and the right output (outcomes) connected with them [5]. The algorithm tries to model the mathematical function that connected these outcomes with the respective inputs. Supervised training responsibilities involve Regression and Classification [40]. Contrary, unsupervised training ensures not to use any output in its training dataset but comprehend interested data entry inside the input data. Reconstruction is atypical category of an unsupervised learning [13]. After the training is end, machine learning models require to be certified by testing to measure their performance evaluation and the evaluation must contain original data, which were not a in the novel training dataset. Or else, the evaluation would be considered intolerant since the model has previously comprehended the dataset. The correct result is considered supervise learning. Also a validation can be carried out to compare diverse output of a parameter.

III. DISCUSSION ON VARIOUS INTRUSION DETECTION TECHNIQUES

There have been a significant number of researches on SDN technology as presented in Table 1 and several of these papers that we have studied are discussed in this section. There are studies which focuses on analysing and evaluating the performance of different SDN controllers and intrusion detection systems using different performance metrics [18]. Some of the synopsis focuses on how to detect and mitigate intrusive attacks across the OpenFlow network through examining traffic behaviour [6]. Different types of cyber-attacks target computer information systems, infrastructures, computer networks using various methods to steal or destroy data or information systems, such as denial of service (DoS) attack, man-in-the-middle attack, SQL injection attack, malware attack etc. [2]. Mechanisms usually used to mitigate these attacks are like black holes, the Intrusion Detection

System (IDS), and advanced techniques such as Deep Packet [11].

Omar et al. [32] mentioned that, Anomaly detection involves supervised techniques and unsupervised techniques and different algorisms are used to attain good result for these techniques. The authors proposed an outline of machine learning techniques for anomaly detection. They also indicate that the supervised learning techniques significantly outperform the unsupervised ones if the experiment data comprises no unknown threats. They showed that multi-layer perceptron, SVM, and the rule-based non-linear techniques achieved great result among the supervised techniques and similarly, K-Means, one class SVM and SOM, achieved better result among unsupervised techniques. The weakness of k-means is that, user has to identify the number of clusters in the beginning and it can only handle numerical data [44]. SVM take long training period for enormous datasets, because it has Challenging to understand and interpret the final model and variable [26]. In case of SOM technique, it requires essential and adequate records in order to improve meaningful clusters [22]. According to [40] there is simplicity of training data in supervised techniques. On the other hand, it has weakness in such a way that it has an inability to learn by itself. Ajaeiya et al. [3] proposed a Flow-Based Intrusion Detection System for SDN and reported that the supervised classifier has the advantage of classifying encrypted flows. The authors showed that the proposed flow-based IDS were able to identify malicious traffic flow with high accuracy measure by F1 score of the classification model and a comparatively low false alarm rate. Al-adaileh et al. [6] proposed a new framework, called SADDCS approach for detecting DDoS attacks. SADDCS is in the category of statistical-based approach for detecting the presence of malicious attack and the authors used this approach for detecting DDoS against the controllers of SDN. The authors, indicated that the proposed design has reduce false positive/negative flow rates, increase detection accuracy and decrease the potentials of targeting SDN controllers across the network. Kaur and Prinima [19] mentioned that, the most important issues in SDN network is the protection of the centre controllers from threat and attack. The authors proposed an optimization algorithm that monitors and analysed the behaviour of network traffic based on detection rate and window size parameters. In the same way, [18] concluded that, to eliminate DDoS attack and improve sequential ratio test, classification techniques will provide accurate result and efficiency would arbitrary distributed through the classification techniques. Mutaz et al. [29] clarifies DDoS attacks and introduced anomaly detection as solitary the well-known detection techniques for intellectual networks.

Hence, narrowing research to DoS attacks only is a problem. It is important to explore different types of attacks with the use of a qualitative dataset in order to prevent and overcome the weaknesses of poor accuracy and high false alert. Al-adaileh et al. [6] have unable to introduce several kinds of attacks thus, applicably only for DDoS Attack. Sangodoyin et al. [36] resolve the issues of DDoS flooding Attack in SDN extensively using Statistical Approach. Proposed and inspire the use of confidence interval and mean throughput in the SDN controller to detect anomaly. This study improves accuracy and reduces overhead. However, leveraged only on throughput for performance evaluation and not convivial to large scale network because, it cantered only to infrastructure layer for attack detection. Ramkumar et al. [33] indicated that, packet overload at the controller result in a single point of failure in SDN. Hence, proposed a Statistical Approach, the mean entropy and window sizes (to control the rate of percentage drop) to prevent the occurrence of DDoS attack. The research reduced detection overhead by controlling the network overloading at the controller. Ajaeiya et al. [3] generate dataset using Python Application and the Dataset established is not adequate enough to covers all areas all types of attacks. Said et al. [35] indicated that, public dataset are tremendously big and comprises many redundant records that appear to be irrelevant for any IDS training.

Huge quantity and qualitative dataset is needed to train machine learning algorithms which is the important aspects of any machine learning algorithm [24]. Certainly, a high-quality dataset can consistently produce improved algorithms on the other hand such datasets are also costly and hard to produce [9]. In the field of intrusion detection there are many dataset available public such as KDD Cup 99, NSL-KDD, CICIDS2017, CSE-CIC-IDS2018, Kyoto2006+, Utwente, UNSW-NB15 etc. Unfortunately, the dataset available have deficiencies and correlated dataset [33]. Most of them have no realistic type attacks or irrelevant to intrusion detection, that is to say, they focused on a particular kind of attack (DoS attack) or different data separately from attack types [31]. This is because, there is no public dataset produced right away from SDN networks architecture and generated purposely for training and evaluation of anomaly detection systems, they are generated for legacy or traditional networks [9], [13]. According to [35] what required as the solution to this problem, is to produce a qualitative and comprehensive SDN dataset and advocate adapting for evaluating the performance of intrusion detection systems. Similarly, to overcome the weakness, applied feature selection methods to produce redundancy-free and reduce irrelevancy dataset for anomaly detection in SDN environment [21]. Reducing the large number of false alerts during the process of detecting unknown attack patterns remains unresolved problem [32]. Consequently, this method of intrusion detection provides poor accuracy and high false alert [33]. That makes the system inefficient and ineffective with poor performance. Problems of distribute denial of service at the Controller and high false positive/negative flow rates is still unsolved and it became a field for research exploration. Al-adaileh et al. [6] proposed Statistical-based Approach by introducing Entropy-based rule and Correlation-based rule to detect DDoS attacks against SDN controllers, reduced false positive/negative rates and also, minimize the complexity of targeting SDN controllers.

ISSN No:-2456-2165

S/N	Reference	Training Dataset	Technique	Attack Type	Evaluation Metrics	Problem	Solution	Strengths	Weaknesses
1	[3]	Self-Made Dataset extracted using Python Application.	Bagged Trees, SVM, Decision Trees, Random Forest and KNN.	DoS, HTTP, Brute force and SSH brute force.	F1 Score and False Alarm.	Challenges of intrusive attacks at the end host.	Proposed an approach of Built-in periodically collected flows' statistics from the OF switches to Classify traffic flow for normal and malicious attacks.	Was able to detect malicious traffic with high accuracy with low false positives.	The system is not adaptive to real time; as such need to be improving for better system transparency. Dataset obtained lack sufficient training dataset that covers all areas to aid in identifying all types of attacks.
2	[6]	No Specific Dataset Introduced.	Statistical-based Approach (Entropy-based rule and Correlation-based rule approaches).	DDoS	Does not indicate evaluation metrics.	Problems of distribute denial of service at the Controller and high false positive/negative flow rates.	Advanced and affirmed a manner for introducing Entropy-based rule and Correlation-based rule to detect DDoS attacks against SDN controllers.	Reduce false positive/negative rates and minimize the complexity of targeting SDN controllers.	Unable to introduce several kinds of attacks. Poor presentation of methodology of the research. Applicably only for DDoS Attack.
3	[19]	Time series dataset, Real Time, Traffic Flow.	Clustered Optimization Technique for machine learning approaches.	DDOS	Threshold Values, Window size and Detection Rate.	Threat and attack targeting and overloading the centre controller.	Advocate the use of optimized technique to Classify and detect malicious traffic flow based on the Statistics of the flow of packets.	Reduce the distribution of the attacks at control layer; decrease the time span of the attacks and improvising detection rate.	Relies on the administrator defined policies to detect attacks. Does not specify threshold values used to assured the effectiveness of the proposed system. Limited to

									DDoS Attack.
4	[34]	NSL-KDD dataset	Classical ML techniques (SVM, J48, Naive Bayes, Random Forest).	Type of attack not indicated.	Precision, Recall, F-score and Accuracy	Concerns that affect the machine learning performance, such as the feature selection methods and the dataset used.	Advocate the use of Deep learning algorithms in detecting Attacks and better results classification.	Indicated that Reduction issues in large-scale dataset make it difficult for machine learning techniques to detect intrusion in SDN network.	Unable to make a distinction on several kinds of attacks. Used non-compatible and outdate datasets
5	[39]	Self-made generated traffic flow.	firewall security system	DDoS	Throughput, Latency, CPU Utilization	Inefficiency on identification and mitigation of attacks in the legacy Network Intrusion Detection Systems (NIDS) on OpenStack Cloud.	Affirmed the use of firewall security system as an efficient Network Intrusion Detection and Mitigation system for OpenStack cloud infrastructures.	Provide better protection and mitigate threats in the infrastructure layer and reduced bandwidth consumption	Takes long time to detect attack. Emphasis to Only infrastructure layer.
6	[25]	Self-made generated traffic flow using hping3 tool.	Snort	DDoS	Round Trip Time and Packet Loss.	Issues affecting the network performance: such as improper data delivery of normal traffic and untimely detection of cyber-attacks based on DDoS.	Proposed the implementation of security system scheme on SDN model, at the client side, can improve the mitigation of DDoS attacks while upholding the standard operation of a network.	Reduces cost, detection overhead of attack traffic and detect and mitigate DDoS without any noticeable packets loss.	Overhead maintenance makes the system complex lead the SDN controller develops threat, taking too much time to mitigate attacks.
7	[28]	Self-Made generated traffic for testing phase Using Scapy tool	Modified K-Means and C4.5 algorithm.	DoS, U2R, R2L and Probe.	Accuracy, Precision, Recall and F-measure.	Inefficiency in keeping track of the network traffic and to detect the malicious	Inveterate the used of flow-based IDS by machine learning classifiers to	Reduced overhead and increase accuracy with low false positive.	Not applicable for large scale Network.

		and NSL-KDD dataset for the training Phase.				activities in the SDN network.	extract essential features of collected traffic flow and classify them to normal and attack nature.		
8	[8]	Self-Made generated traffic Dataset.	Credit-Based Threshold Random Walk (CB-TRW), Rate Limiting (RL) and Port Bingo (PB) algorithm.	Port-scanning and Denial of Service (DoS) attacks.	Percentage CPU usage and False Positives Alerts	Issues of accessing sensitive Data and security policy violations.	Proposed an Intrusion Detection and Prevention System (IDPS) using SDN to detect and mitigate attacks by protecting against port-scanning and Denial of Service (DoS) attacks.	Reduced Bandwidth consumption of attack traffic and reasonable resource utilization. Provides efficiency and real-time protection against cyber attacks	Relies on the administrator defined policies to detect attacks.
9	[21]	NSL-KDD dataset	J48, Random Forest, Projective Adaptive Resonance Theory (PART), Naive Bayes, Decision Table (DT), Radial Basis Function Network (RBFN), and Bayesian Network.	DDoS	Accuracy (AC), precision (P), recall (R), F-measure (F), False Alarm Rate (FAR), and Mathews correlation coefficient (MCC).	Ineffectiveness of machine learning classifiers in classifying data.	Applied feature selection methods are applied as data pre-processing to produce redundancy-free data set for anomaly detection in SDN environment.	Quick response to attack and increase accuracy and low false positive.	Unable to make a distinction on several kinds of attacks. Used non-compatible and outdate datasets
10	[5]	ISCXIDS2012 dataset	Deep learning algorithm: Long-Short-Term Memory (LSTM), Recurrent Neural Networks (RNN).	Distributed Denial of Service Botnet, Brute-Force, L2L, L2R, R2L and R2R.	Confusion Matrix, ROC, F-1 Score, Accuracy, Precision and Recall.	Issues of scalable security threats in control layer.	Proposed a Deep learning approach using long short-term memory (LSTM) to overcome the scalable security issues,	Provide Smart Intrusion Detection System that offer scalable threat detection and improve accuracy in SDN.	Used non-compatible and outdate datasets

							detection and mitigation in control layer.		
11	[33]	Scapy is used for generating data traffic.	Statistical Approach: mean entropy and window sizes.	DDoS	Packet loss and Detection Rate.	Issues of packet overload at the controller resulting in a single point of failure.	Proposed the use of mean entropy and the rate of percentage drop to prevent the occurrence of DDoS attack.	Reduced detection overhead by controlling the network overloading at the controller.	Restricted to DDoS Attack. Not applicable for large scale network. Poor accuracy and high false alert.
12	[9]	KDD 99	Fuzzy logic	DOS and DDoS.	CV SCORE	Issues of Do vulnerability and difficulty in segregating between ordinary behaviour and anomalous behaviour.	Proposed and encouraged the use of Fuzzy Logic for attack detection and better expectation of attacks in small scale network.	Reduced bandwidth consumption and provide assistances in well identification of interference in SDN.	Relies on low quality training datasets. Make the system complex.
13	[18]	Self-Made generated traffic Dataset.	Self-Organizing Maps and Learning Vector Quantization.	DoS, U2R, R2L and Probe.	False Positive Rate and True Positive Rate.	Issues of monitoring and detection of malicious activities in the SDN data Layer.	Introduced an efficient and effective Intrusion detection environment for training phase to classify and validate using machine learning algorithms.	Improved the efficiency of detection of U2R attacks and reduced resource utilization.	Processing overhead not discussed. Focussed to threat on Infrastructure layer.
14	[27]	Scapy is used for generating data traffic.	Entropy-based and C4.5 technique.	DDoS flooding	Sensitivity, specificity and accuracy.	Problem of DDoS attack flooding and overload the SDN controller and switch flow table.	proposed two level security mechanisms : entropy-based mechanism and machine learning-based C4.5 technique to detect the DDoS flooding attack and drop the	Improve the accuracy, provide low false alert rate and reduce the problem of overhead at the control Layer.	Applicable to only DDoS flooding attack. Cause enormous number of disorder in SDN environment because of DDoS Attack.

							packets.		
15	[17]	Self-Made generated traffic Dataset.	Self-organizing Maps	DoS, U2R, R2L and Probe.	Not Indicated.	Problem of unauthorized activities in SDN.	Proposed a measurement system that assemble network traffic flow factors and used in machine learning methods to detect unauthorized activities.	Quick response to attack.	Processing overhead not mentioned. Evaluation of the performance metrics is not shown.
16	[35]	Self-Made generated traffic Dataset.	Decision Tree, Random Forest, Adaptive Boosting, k-nearest Neighbour classifier, Naive Bayes, Support Vector Machines, Linear kernel, radial basis function kernel and multilayer perceptron model.	Botnet, DoS, DDoS, Password Brute-Forcing attack and probe.	Precision, recall, precision and F-score.	Most of the of the published researches use non-compatible and out-dated Datasets which cannot be used directly for anomaly detection in SDN.	Produce a qualitative and comprehensive SDN dataset and advocate adapting for evaluating the performance of intrusion detection systems.	Completely transparent and quick response to numerous kinds of attacks.	Applicable to only one controller, need to be enhance for large scale network to cover all network nodes and users.
17	[7]	NSL-KDD dataset	Deep Learning Approach: Deep Neural Network (DNN) and Gated Recurrent Neural Network (GRU-RNN),	DoS, U2R, R2L and Probe.	Accuracy, Precision, Recall), and F1-measure, throughput, latency, and resource utilization.	Vulnerability affects the performance of the OpenFlow controller.	Propose a deep learning (DL) approach for a network intrusion detection system in the SDN architecture.	Does not distress the performance of the OpenFlow controller, reduces bandwidth consumption and resource utilization and provide better accuracy.	Low detection rate and high false alarm rate. Processing overhead not discussed.
18	[24]	Python script is used to generate attack and benign traffic with the Scapy tool.	Stacked Auto Encoder (SAE) and Convolutional Neural Network (CNN).	DDoS	Precision (P), Recall (R), and F1-measure (F1),	There are problems to separate and manage among the sophisticated traffic volume of a DDoS attack and bulky	Proposed effective and efficient entropy-based DDoS detection appropriate to covenant with considerably	Reduces network traffic overhead. Improve higher detection rate, accuracy and low false positive	Limited to DDoS Attack.

						number of authentic users accessing a network resource.	immense DDoS traffic flow in a SDN.	alerts.	
19	[31]	Self-Made generated traffic Dataset	Deep Learning	DDoS	Precision, Recall, and F1-measure, Receiver Operating Curve (ROC).	Issues of predominant DDoS attacks that affect organizational network infrastructure.	Proposed a deep learning based multi-vector DDoS detection system in SDN.	Increase accuracy with a low false-positive for attack detection.	Approach constraints the controller's performance and used non-compatible generated traffic Data.
20	[13]	CICIDS2017	Deep CNN Ensemble Framework: RNN, LSTM, RL and CNN.	DDoS	Precision, Recall, Accuracy and F1-measure.	Problem of sophisticated and conventional DDoS attack emerging in SDN.	Proposed an efficient, competent, scalable and early detection of large-scale sophisticated DDoS attacks deep Using CNN ensemble scheme.	Improves detection accuracy and computational difficulty.	Non-compatible and out-dated Datasets. Limited to DDoS Attack.
21	[36]	Self-Made generated traffic Dataset	Statistical Approach: Confidence interval and mean Throughput.	DDoS, TCP ACK Flood and TCP SYN Flood.	Throughput	Problem of DDoS flooding Attack in SDN.	Proposed and Inspire the use of confidence interval and mean throughput in the SDN controller to detect anomaly.	Improves accuracy and reduced overhead.	Leveraged only on throughput for performance evaluation. Not convivial to large scale network because, it cantered only to infrastructure layer for attack detection.
23	[1]	Self-Made generated traffic Dataset.	Firewall rules.	DoS	Round Trip Time (RTT), latency (jitter), bandwidth and throughput.	Issue of Denial of Service (DoS) attack resulted as a result of packets flooded from an attacker to access the	Proposed a scheme to evaluate the performances of the controllers against DoS attack in respect to user	Completely transparent and reasonable resource consumption.	Applicable to only DoS attacks. A single controller is used thus, not applicable for large

ISSN No:-2456-2165

						controller.	datagram protocol (UDP) and transmission control protocol (TCP).		network. Relies on firewall rules to detect an attack. Used non-compatible generated traffic Data. Resources consumption in the controller due to packet overload.

Table 1:- Comparison of Various Research Works based on SDN

Recently, research challenges regarding network security and rapid advancement of network operability have made research group to adventure their knowledge into the emerging SDN Technology. Said et al. [34] introduced an efficient benchmarking examination of the recent machine learning techniques for the detection of malicious traffic activities in SDNs. The authors empirically demonstrated and experiments on an openly accessible dataset of Intrusion Detection Systems (IDSs) called NSL-KDD dataset and concluded that traditional machine-learning based techniques fail to have a better performance compare to classical machine learning based techniques. Sooraj and Prabhakar [39] proposed an SDNFV based security structure in an extensive OpenStack cloud environment, for attack detection and prevention, security investigation and threat analysis. The authors introduced the framework that provides attack identification and mitigation (e.g. DDoS attack). This proposed framework, improved quality of service when compare to legacy IDS solution. Manso et al. [25] proposed an IDS framework for detecting and preventing and intrusive attacks. The IDS is designed with a module for attack detection and the IDS will sent an alert to controller when malicious activities are detected and the controller forward the alert to switch to prevent such attacks for future occurrence. Muthamil and Deepalakshmi (2019) mentioned that, to solve security issues concerning SDN network, they proposed a Flow Based Intrusion Detection System using machine learning model to detect an intrusive attacks. This hybrid machine learning technique is an extension or modification of K-Means and C4.5 Algorithm. The authors noted that the experiment result indicated that proposed work can categorize the normal and malicious occurrences with accuracy of 97.66%. Birkinshaw et al. [8] designed and implement an implement an Intrusion Detection and Prevention System (IDPS) for detecting and defending malicious activities e.g. DDoS, security policy destruction and port scanning attacks by monitoring network traffic flow in SDN environment. The authors in-cooperated Rate Limiting (RL) techniques, Credit-Based Threshold Random Walk (CB-TRW) techniques and Port Bingo (PB) algorithm within the IDPS as a method to defend against attacks. The authors reported that, the proposed design has high potential for detecting and stopping real-time attacks and reducing the rate of false positive by turning down the values of threshold within the detection algorithm. Ahmed et al. [1] is dedicated to simulate and observe the influence of DoS attack on the bandwidth in an SDN network. Also, established and emulated SDN network by using several testing tools. The authors analysed and evaluated the Network performance of how it can affect the bandwidth and latency (jitter) of DoS attack on SDN network. Additionally, noted that, DoS attack have an impact upon the controller by initiating flood of packets. The authors have not proposed any techniques for intrusions detection and prevention. Most of the existing works has focused on detecting attacks using data streaming approach, Deep learning, machine learning approach and data mining approach in SDN-based OpenFlow network. Kumar et al. [21] discussed that Machine learning techniques (ML) can be applied to improve detection accuracy and low false alarm rate to improved system performance and better intrusion detection. According to [34] deep learning is getting attention on intrusion detection and not only intrusion detection region but every aspect of face detection, speech recognition and image processing has been covered by deep learning technique. These deep learning methods are yet to attain a high standard accuracy but machine learning have reached nearly 99% of accuracy.

As a final point, considering different research papers presented and reviewed on SDN based intrusion detection techniques, there are still SDN security and performance challenges that need to be address to produce robust, secure and reliable SDN network. Al-adaileh et al. [6] identify that it is an unreliable method using a single controller in an SDN environment to detect intrusive attacks. Suresh et al. [41] also indicated that qualitative and comprehensive SDN dataset with numerous type of attack is required in obtaining efficient result on identifying intrusion detection. Ajiya et al. [4] proposed an effective and efficient solution model for intrusion detection system using machine learning

approached on SDN environment. The author introduced the used of multiple controllers to tackle new incoming packets and feature selection methods to produced redundancy-free and reduced irrelevancy dataset for anomaly detection in SDN environments. The author lastly indicated that the model will improve performance and security by producing high detection rate and low false alarm rate.

IV. CONCLUSION

In this article, we provided an overview of different types of intrusion detection system with various defence mechanisms involved and studied the emerging technology of Software-Defined Networking (SDN). Also, surveyed and outlined various research works on intrusion detections techniques and highlighted their strengths and weakness. Based on this comparative analysis of various research works, it is concluded that the novel machine learning approach can simply and effectively applied to detect vulnerabilities and monitor networks traffic flow in SDN.

REFERENCES

[1]. Ahmed, F. A., Fatty, M. S., Ashraf, T. and Mohamed, H A. (2020). Performance Analysis and Evaluation of Software Defined Networking Controllers against Denial of Service Attacks. Journal of Physics: Conference Series.Conf. Ser. 1447 012007.

[2]. Ahmed, M., Abdun, N. M., Jiankun, H. (2016).A survey of network anomaly detection techniques.Journal of Network and Computer Applications. 60, 19-31.

[3]. Ajaeiya, G. A., Nareg, A. Imad, H. E., Ayman, K. and Ali, C. (2017).Flow-Based Intrusion Detection System for SDN.IEEE Symposium on Computers and Communications (ISCC).1, 17, 787-793.

[4]. Ajiya, A. A., Musa, A. B. and Aliyu, M. M. (2021). Solution Model for Intrusion Detection in Software Defined Networking (SDN) using Machine Learning. Quest Journals: Journal of Software Engineering and Simulation, Volume 7,Issue 8, pp: 40-47.

[5]. Akhunzada,A., Iram, B., Jahanzaib, M. and Tanzila, S.(2019). Intelligent intrusion detection systemusing deep learning in Software defined network. https://www.researchgate.net/publication/341756680.

[6]. Al-adaileh, M., A. A., Mohammed, A., Yung-Wey, C., and Ahmed, A. (2018). Proposed statistical-based approach for detecting distribute denial of service against the controller of software defined network (SADDCS). MATEC Web of Conferences.218, 02012.https://doi.org/10.1051/matecconf/201821802012.

[7]. Anh, T. T., Lotfi, M., Des, M., Syed, A. R. Z., Mounir, G. and Fadi, E. (2020). DeepIDS: Deep Learning Approach for Intrusion Detection in Software Defined Networking. Electronics: MDPI. DOI: 10.3390/electronics9091533.

[8]. Birkinshaw, C., Rouka, E. and Vassilakis, V. (2019). Implementing an Intrusion Detection and Prevention System Using Software-Defined Networking: Defending Against Port-Scanning and Denial-of-Service Attacks. Journal of Network and Computer Applications.136. 10.1016/j.jnca.2019.03.005.

[9]. Budugutta, S.and Nithya, S. (2017).Intrusion Detection using fuzzy logic in Software Defined Networking. International Conference on Intelligent Computing Systems (ICICS).Pp.102 – 108.

[10]. Chellani, N., Prateek, T., Prashant, H. and Vishal, N. (2016). Enhancing Security in OpenFlow Capstone Research Project Proposal.1-10.

[11]. Galeano, J. B., Javier, C. M., Juan, F. V. and Francisco, L. (2020). Detection and Mitigation of DoS and DDoS Attacks in IoT-Based Stateful SDN: An Experimental Approach. MDPI: Sensors — Open Access Journal. 20, 816, 2-18.

[12]. Giotis, K., Argyropoulos, C., Androulidakis, G., Kalogeras, D., and Maglaris, V. (2013).Combining OpenFlow and sFlow for an effective and scalable Anomaly Detection and Mitigation mechanism on SDN Environments, Computer Networks.

[13]. Haider, S., Adnan, A., Iqra, M., Tanil, B., Amanda, F., Kim-kwang, R. C. and Javed, I. (2020).A Deep CNN Ensemble Framework for Efficient DDoS Attack Detection in Software Defined Networks. Volume 4, DOI: 10.1109/ACCESS.2020.2976908, IEEE Access.

[14]. Hakiri, A., Aniruddha G., Pascal B., Douglas C. S.t, and Thierry G. (2014). Software-defined networking: Challenges and research opportunities for future internet. Computer Networks. 75, 453–471. DOI:http://dx.doi.org/10.1016/j.comnet.2014.10.015.

[15]. Hand, R., Ton, M., and Keller, E. (2013) "Active Security," ACM SIGCOMM Hot Topics in Networks.

[16]. Husham, B. A. A. (2017). Detection of DDoS Attacks against the SDN Controller using Statistical Approaches.(Master's Theses, Wright State University, 2017).Theses and dissertations CORE Scholar.

[17]. Jankowski, D. and Marek, A. (2015).Intrusion Detection in Software Defined Networks with Self-organized Maps. Institute of Telecommunication, Faculty of Electronics, Military University of Technology.

[18]. Jankowski, D. and Marek, A. (2016). On Efficiency of Selected Machine Learning Algorithms for Intrusion Detection in Software Defined Networks. International Journal of Electronics and Telecommunications. VOL. 62, No. 3, pp. 247-252. DOI: 10.1515/eletel-2016-0033.

[19]. Kaur, G. and Prinima, G. (2018).Proposed Optimization Technique to detect DDOS Attacks on Software Defined Networks.4th International Conference on Computers and Management (ICCM).281-287.

[20]. Kumar, G. (2014). Evaluation Metrics for Intrusion Detection Systems - A Study.International Journal of Computer Science and Mobile Applications. 2, 11, 11-17.

[21]. Kumar, S. D., Raihan, U. and Mahbubur, R. (2020). Performance Analysis of SDN-Based Intrusion Detection Model with Feature Selection Approach. International Joint Conference on Computational Intelligence, Algorithms for Intelligent.pp.483 494.

[22]. Kunal, S., Gandhi, P., Sutariya, R. and Tarpara, H.(2020). A secure software defined networking for distributed environment. Security and Privacy.https://doi.org/10.1002/spy2.130.

[23]. Lakshmanan, A. (2018).Enhanced Software Defined Networking (SDN) with security &performance in cloud computing. https://www.researchgate.net/publication/329735894.

[24]. Majid, R. A. U., Zeeshan, P., Keshav, D., Wajahat, A., Asad, M. K. and Bashir, H. (2021). Entropy Based Features Distribution for Anti-DDoS Modelin SDN. Sustainability: MDPI.https://doi.org/10.3390/su13031522.

[25]. Manso, P., Jose, M. and Carlos, S. (2019). SDN-Based Intrusion Detection System for Early Detection and Mitigation of DDoS Attacks.Information-Open Access Journal.10.106.1-17.

[26]. Mehdi, S. A., Khalid, J., and Khayam, S. A. (2011). "Revisiting traffic anomaly detection using software defined networking," Recent Advances in Intrusion Detection. Springer, pp. 161–180.

[27]. Muthamil, K. S. and Deepalakshm, P. (2020).A two level security mechanism to detect a DDoS flooding attack in software-defined networks using entropy-based and C4.5 technique.Journal of High Speed Networks. No. 26, pp 55–76. DOI 10.3233/JHS-200630.

[28]. Muthamil, K. S. and Deepalakshmi, P. (2019). Flow Based Intrusion Detection System for Software Defined Networking using Hybrid Machine Learning Technique. International Journal of Innovative Technology and Exploring Engineering (IJITEE). 9, 2S2, 1026-1033.

[29]. Mutaz, H. H. K., Sharifah, H. S. A., Abdul,Latiff, N. M., Abdullah, A. S. and Hassan, M. K. (2018). A Review of Anomaly Detection Techniques and Distributed Denial of Service (DDoS) on Software Defined Network (SDN).Engineering, Technology & Applied Science Research. Vol. 8, No. 2, pp. 2724-2730.

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

[31]. Niyaz, Q., Weiqing, S. and Ahmad, Y. J. (2016). A Deep Learning Based DDoS Detection System in Software-Defined Networking (SDN). https://www.researchgate.net/publication/310671661.

[32]. Omar, S., Asri, N.and Hamid, H. J.(2013). Machine Learning Techniques for Anomaly Detection: An Overview. International Journal of Computer Applications (0975 – 8887). 79, 2, 33-35.

[33]. Ramkumar, M. P., Emil, S. and Bavani, K. (2020).Statistical Approach Based Detection of Distributed Denial of Service Attack in a Software Defined.International Conference on Advanced Computing & Communication Systems (ICACCS).No. 6.pp. 380 -385.

[34]. Said, M. E., Nhien-An, L., Soumyabrata, D. and Anca, D. J. (2019). Machine-Learning Techniques for Detecting Attacks in SDN.ArXiv, open-access repository of electronic preprints.

[35]. Said, M. E., Nhien-An, L. and Anca, J. (2020). InSDN: A Novel SDN Intrusion Dataset. DOI10.1109/ACCESS.2020.3022633, IEEE Acces

[36]. Sangodoyin, A., Babagana, M., Irfan, A., Jules, P. D. (2018). An approach to detecting distributed denial of service attacks in software defined Networks. International Conference on Future Internet of Things and Cloud.DOI 10.1109/FiCloud.2018.00069. pp. 436 – 443.

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

[38]. Skowyra, R., Bahargam, S., and Bestavros, A.(2013). "SoftwareDefined IDS for Securing Embedded Mobile Devices,".[Online]. Available: http://www.cs.bu.edu/techreports/pdf/2013-005-software-defined-ids.pdf.

[39]. Sooraj, V. H. and Prabhakar, K. (2019). SDN based Intrusion Detection System for OpenStack Cloud. International Journal of Innovative Technology and Exploring Engineering (IJITEE). 8, 9, 2443-2449.

[40]. Sultana, N., Naveen, C., Wei, P. and Rabei, A. (2018). Survey on SDN based network intrusion detection system using machine learning approaches.Peer-to-Peer Networking and Applications.https://doi.org/10.1007/s12083-017-0630-0

[41]. Suresh K., Tarun K., Ganesh S. and Maninder S. N. (2012). Open Flow Switch with Intrusion Detection System. International Journal of Scientific Research Engineering & Technology (IJSRET), 1, 7. pp 001-004.

[42]. Tantar, E., Palattella, M. R., Avanesov, T., Kantor, M., and Engel, T. (2014). Cognition: A Tool for Reinforcing Security in Software Defined Networks, ser. EVOLVE-A Bridge between Probability, Set Oriented Numerics, and Evolutionary Computation V. Springer, pp. 61–78.

[43]. Wang, Y., Zhang, Y., Singh, V., Lumezanu, C., and Jiang, G. (2013) "NetFuse: Short-circuiting traffic surges in the cloud,"IEEE International Conference on Communications (ICC). IEEE, pp. 3514–3518.

[44]. Xing, T., Huang, D., Xu, L., Chung, C.J., and Khatkar, P. (2013)."Snortflow: Aopenflow-based intrusion prevention system in cloud environment," Research and Educational Experiment Workshop (GREE), 2013 Second GENI. IEEE, pp. 89–92.

[45]. Zaalouk, A., Khondoker, R., Marx, R., and Bayarou, K. (2014). "OrchSec: An orchestrator-based architecture for enhancing network-security using Network Monitoring and SDN Control functions," Network Operations and Management Symposium (NOMS), IEEE. IEEE, 2014, pp. 1–9.