Journal of Parallel and Distributed Computing 154 (2021) 142–152

Contents lists available at ScienceDirect

J. Parallel Distrib. Comput.

journal homepage: www.elsevier.com/locate/jpdc

Rival-Model Penalized Self-Organizing Map enforced DDoS attack prevention mechanism for software defined network-based cloud computing environment

Pillutla Harikrishna [a,*], A. Amuthan [b]

[a] Department of Computer Science and Engineering, Rajeev Gandhi Memorial College of Engineering and Technology, Nandyal, India
[b] Department of Computer Science and Engineering, Pondicherry Engineering College, Puducherry, India

ARTICLE INFO

Article history:
Received 7 March 2020
Received in revised form 25 January 2021
Accepted 13 March 2021
Available online 31 March 2021

Keywords:
Software Defined Networking
Cloud computing
Rival-Model Penalized Self-Organizing Map (RMPSOM)
DDoS attacks
Learning rate

ABSTRACT

Reliability, and safety are considered as the indispensable twins during the adoption of the cloud computing environment since their breaches lead to catastrophic issues in poor resource management and unreliable service quality. To be specific, Distributed Denial of Service (DDoS) attack is determined as the most vulnerable threat in the cloud space as it lowers the ability of the predominant resources' for preventing their optimal utilization. The advent of Software-Defined Networking (SDN) is estimated to wide open the feasibility in preventing DDoS attacks in the cloud space. In this paper, a Rival-Model Penalized Self-Organizing Map (RMP-SOM) enforced DDoS Attack Prevention Mechanism is proposed for the remarkable prevention of DDoS attack by utilizing the potential characteristics of SDN that focuses on the possibility of facilitating network global perspective, effective investigation of network traffic, and an enhanced process of rule updating. This proposed RMPSOM-SDNDM scheme utilizes the benefits of the constant rate in order to ensure priority to the closest neuron and its neighborhood rather than its farthest rival neuron for facilitating better detection accuracy. The simulation results of the proposed RMPSOM approach confirmed a phenomenal sensitivity, specificity and accuracy rate during the process of detecting DDoS attacks in the cloud space on par with the baseline DDoS mitigation schemes considered from the literature.

1. Introduction

In a cloud computing environment, security issues are considered to be the highest concern to a diversified number of stakeholders in order to enable them in deciding on an appropriate method of adoption [1]. In the recent past, a considerable number of researchers have focused on the cybersecurity issue intending to revise the cloud space such that they do not influence the resource management, service quality, and budget of the cloud computing environment [2]. To be specific, Distributed Denial of Service (DDoS) attack is considered as the most vulnerable security issue in the cloud space since it compromises the host to forward a huge amount of data to the targeted victims [3]. This compromise of the hosts is mainly for depleting server bandwidth, unnecessary utilization of the cloud computing resources, and for introducing imbalance in the synchronization between cloud entities to a maximum level [4]. Generally, DDoS attacks target the server to hurdle its service provisioned to the consumers of the cloud environment [5]. Then, the DDoS attackers disguised as legitimate customers flood the interacting server to a maximum degree such that maximum services are made unavailable because of the large number of requests that remain unprocessed leading to the overflow condition of queue service [6]. To be specific, DDoS attackers correspond to the collection of machines that concentrates on crumbling the services of the existing resources by unnecessary exhaustion of focused service. Further, a significant number of proofs also inferred the target shift of DDoS attacks to the cloud infrastructures and services. Several prevention approaches were proposed in the literature in the recent decade for handling the impacts of the DDoS attack on the cloud computing environment [7]. The emergence and the recent advent in Software-Defined Networking (SDN) during recent years also proved to increase the viability in preventing the DDoS attack in the cloud computing environment [7]. Thus, the SDN-based cloud service provision enhances the possibility of defeating DDoS attacks in the cloud environment. However, a kind of contradictory association exists between the SDN and the DDoS attack in the cloud environment since the SDN focuses on centralized control, software-oriented traffic analysis, dynamic and reactive forwarding rule enhancement for detecting and reacting to the degree of influence imposed by the attackers [8]. At

[*] Corresponding author.
E-mail address: pillutlaharikrishna@yahoo.co.in (P. Harikrishna).

https://doi.org/10.1016/j.jpdc.2021.03.005
0743-7315/© 2021 Elsevier Inc. All rights reserved.

the same time, the security of SDN is another issue that needs to be addressed since the DDoS category of attacks are also possible in the SDNs. The recent contributions to the literature enhance the probability of including the characteristic merits of different variants of Self Organizing Maps (SOM) to investigate the traffic flow in the cloud environment [9]. This inclusion of different variants of SOM was confirmed to improve the security of the SDN as well the security of the incorporated cloud computing environment with the view to improve the centralized control, software-oriented traffic analysis, dynamic and reactive forwarding rule enhancement for preventing the DDoS attackers in the cloud environment [10].

In this paper, Rival-Model Penalized Self-Organizing Map using Software Defined Network (RMPSOM-SDNDM) is proposed for enforcing DDoS attack prevention in a cloud computing environment. This proposed RMPSOM-SDNDM scheme focuses on the preservation of the topological structure of the input data by considering the maximum similarity quantified based on Euclidean distance. This quantification of the similar probabilistic data traffic flow factors aids in potential mapping to the neighboring neurons in the RMPSOM for facilitating superior and reliable detection of DDoS in the cloud environment. The constant learning rate in the proposed RMPSOM-SDNDM scheme is mainly used for improving the adaptation necessary in classifying the monitored traffic flows into normal and malicious. The simulation experiments of the proposed RMPSOM-SDNDM scheme are investigated for quantifying its excellence based on detection accuracy under different False Positive rate by varying the data rates. Further, the potential of the proposed RMPSOM-SDNDM scheme is also explored based on the False Positive rate, True Positive rate, and True Negative rate under different intensities of data rate. Besides, the excellence of the proposed RMPSOM-SDNDM scheme is also investigated using True Positive Rate by varying the data rates under the impact of varying intensities of False Positive rate.

The major contributions of the proposed RMPSOM-SDNDM scheme are listed as follows.

(i) It is proposed with a significant learning algorithm that adaptively selects different arrivals of each input among the best-matching unit with the penalization of their related models during the classification process of data traffic flows.
(ii) It is the potential classification scheme proposed for better classification between normal and malicious data traffic in SDN based on the merits of RSOM.
(iii) It is proposed with the benefits of neurons that are employed in the process of estimating the Euclidean distance between the actual data traffic with the expected data traffic in order to prevent DDoS attacks in the cloud space.
(iv) It included a constant learning rate that prevents the worst selection of a monotonically decreasing function for the purpose of attaining robust classification.

The forthcoming sections of the paper are organized as follows. Section 2 presents a potent review of the most recent contributions proposed in the literature for mitigating DDoS attacks in the cloud environment. Section 3 highlights the detailed view of the proposed RMPSOM-SDNDM scheme with its characteristics, merits, and role in detecting and preventing DDoS attacks in the cloud space. Section 4 exemplars the simulation results of the proposed RMPSOM-SDNDM scheme evaluated under the detection accuracy, False Positive rate, True Positive rate, and True Negative rate under different intensities of data rate. Section 5 concludes the paper with major contributions and the scope of future research.

2. Related work

Initially, a DDoS attack mitigation framework named Athena was proposed using SDN for detecting anomaly misbehavior tasks in a cloud computing environment [11]. This Athena mitigation framework was proposed as a complete mitigation architecture for facilitating an improved degree of scalability. The detection accuracy of this Athena framework was determined to be predominant since it uses the benefits of the control plane and data plane for superior mitigation. Another, SDN-based DDoS attack mitigation mechanism was contributed for improving the possibility of detection and rapid isolation of traffic flow from cloud computing [12]. The detection accuracy of this SDN-based DDoS attack mitigation mechanism was estimated to be excellent since it possesses adaptive response in categorizing flow into genuine and attack flows depending on the kind of data traffic flow. The False Positive rate of this SDN-based DDoS attack mitigation mechanism was estimated to be better than the comparable Athena Framework. A Transmission Control Protocol (TCP)-based DDoS attack mitigation scheme was proposed using SYN cookies for eliminating the influence of attack in the cloud server [13]. This TCP-based DDoS attack mitigation scheme prevents the DDoS attacks by monitoring the proxy, false and duplicate acknowledgment generated from the client. This TCP-based DDoS attack mitigation approach uses dual layers of security in which several rules are investigated for classifying the genuineness. This TCP-based DDoS attack mitigation approach also used the Message Authentication Code (MAC) for facilitating superior security in the cloud computing environment.

Further, a DDoS attack prevention scheme using virtualization of network function and benefits of SDN was proposed for categorizing the traffic flows into genuine and malicious [14]. This DDoS attack prevention scheme using network function virtualization enhances the possibility of detection by using a lightweight probing method. This lightweight probing method incorporation was utilized for assigning a virtual scrubbing factor that aids in reducing the network delay, with the possibility of approaching the victim of DDoS attack under reduced network proof that is left between the attacks. This DDoS attack prevention scheme facilitated an improved response time by 96.79% during its evaluation under the design of the proof of concept approach. An SDN-based DDoS attack detection framework called DELTA was proposed for identifying, standardizing, and automating the process of eliminating weakness that results in the SDNs. This DELTA framework possesses the options of re-instantiating different SDN attacks in a number of implementation environments. This DELTA framework also utilized a fuzzy module that aids in the automatic discovery of weaknesses that emerge during the control of hosts in the cloud environment. The Detection Accuracy, Precision, and the Recall value of this DELTA framework were determined to be maximum with a reduced False Positive rate [15]. Then, a Hop Count Filter Approach (HCFA) was contributed to strengthening the process of detecting DDoS attacks through the benefits of SDNs [16]. This HCFA scheme was determined to ensure maximum protection by blocking spoofed packets from the cloud with improved response and Detection Accuracy rate. This HCFA scheme was estimated to enhance the response rate to a maximum of 98.21% compared to the DELTA and Athena mitigation methods of the literature. The Precision and Recall values with minimized False Positive rate were identified due to the derivation of the hop count filter that aids in the accurate classification of data traffic flows into normal and malicious. A Bloom Filter-based DDoS Control Framework Model (BF-DCFM) was proposed for inclusion into the SDN for defeating the issues that are introduced due to the inclusion of DDoS attacks in the cloud environment [17]. To be specific, this BF-DCFM was capable of resolving the crucial issues of the link flooding category of DDoS attacks. This BF-DCFM method of integrating bloom filter and SDN utilized two modules for detecting link flooding category of DDoS attacks in order to facilitate maximum detection accuracy with minimized overhead. The response time enabled by this BF-DCFM was also maximum since it is able to achieve higher Precision and Recall values. A FRESCO-based Detection Mechanism (FRESCODM) for handling DDoS attacks was contributed for determining malicious flow using the benefits of fuzzy mapping tool [18]. This FRESCODM approach was proposed for handling DDoS attacks in any category of OpenFlow scenario such that benefits of click under data traffic monitoring is sustained to the maximum degree. A Trusted Random Walk-based Fuzzy Logic Imposed Detection Mechanism (TRW-FLIBDM) was proposed for significant detection of DDoS attacks in the cloud environment [19]. The trusted random walk aimed at categorizing the data traffic flow in a significant manner such that appropriateness in classifying data traffic is enhanced phenomenally. The response rate of TRW-FLIBDM was determined to be maximized on par with the BF-DCFM and FRESCODM schemes of the literature. Finally, the authors also proposed a Fuzzy Self Organizing Map-based SDN detection Mechanism (FSOM-SDNDM) for enhancing the rate of estimating data traffic flows in the cloud into normal and malicious [20]. This FSOM-SDNDM is an improved neural network model that is an enhancement over the classical Kohenen network based on its dynamic property with the enhanced process of reactively updating fuzzy rules. The FSOM-SDNDM approach incorporates fuzzy rules for investigating the perspectives of input space for mapping them into single-valued output in order to facilitate the option of DDoS attacks in the cloud environment. The incorporation of control plane benefits in SDN was determined to improve the attack response approach in this FSOM-SDNDM approach to the maximum level compared to the existing FRESCODM and TRW-FLIBDM schemes. The Classification Accuracy and Precision of this FSOM-SDNDM approach were estimated to be 94% and 93.87% under its evaluation with the different intensities of false positive rates.

A Dual address entropy-based DDoS attack detection and defense scheme was proposed with the merits of cognition-based computing that classifies malicious data flows from normal data flows [21]. This dual address entropy detection scheme was proposed with the merits of extracting the flow table characteristics and attack models that are constructed with the benefits of support vector machine. It was proposed with the properties that realize the detection and mitigation process that can restore normal communication in a real-time scenario. The results of this dual address entropy detection scheme confirmed a low false positive rate and high detection rate. The time incurred in the recovery of the DDoS attack facilitated by this scheme was also determined to be better than the existing algorithms of the literature. An Advanced Support Vector Machine (ASVM)-based DDoS defense scheme was proposed as an SDN-based strategy that performed multi-classification of data traffic flows [22]. It was proposed for the successful detection of two categories of flooding-based attacks. It utilized the predominant features of asymmetric and volumetric for minimizing the training and testing time involved in the data traffic classification process. The results of this AVSM-based DDoS defense scheme confirmed better accuracy of 97.21%, a detection rate of 98.38% and a reduced false alarm rate of 11.49%, compared to the baseline schemes.

In addition, the SNORT intrusion detection system for DDoS attack detection was proposed with the benefits of networking operating systems and an Open Daylight-based controller for better discrimination between data traffic flows [23]. This mitigation approach used Wireshark for bombarding the data traffic towards the controllers in order to perform evaluations of packets in the SDN controller. This SNORT approach was determined to be better in terms of reducing the percentage of packet loss, round trip time, and time incurred in detecting DDoS attacks at the SDN controller. It was identified to incur minimum time in detecting successful DDoS attacks in the SDN network. An integrated DDoS defense mechanism was proposed using the machine learning algorithms such as random forest, decision tree, MLP, and SVM for classifying malicious data traffic and normal data flows [24]. The proposed defense scheme utilized the merits of the Scapy tool for simulating DDoS attacks based on the acquirement of a valid list of IPs. This context defense scheme attained the best accuracy and optimal processing time with respect to random forest and decision algorithm implementation. It was considered to be potent in classifying DDoS attacks by capturing the most significant features that aided in classifying bandwidth attack, flow-table attack, and controller attack from the complete set of data traffic flows that propagates through the SDN controller. An SDN-based DDoS attack detection scheme was proposed for exploring the features in order to minimize the data bias involved in the detection process [25]. The potential of the defense scheme was explored using the dataset of Knowledge Discovery and Data Mining Tools Competition (KDDCUP) 99 datasets confirmed better performance compared to SVM in the SDN network [26].

Extract of the literature

The main limitations of the existing works of the literature that motivated the formulation of the proposed RMPSOM enforced DDoS Attack Prevention Mechanism are presented as follows.

(i) Most of the existing self organizing schemes failed in utilizing a constant learning rate that has the possibility of preventing the impotent selection of monotonically decreased function that decreases the accuracy in detection.
(ii) The classification accuracy achieved by most of the learning algorithms-based DDoS defense scheme was considered to still possess a room for improvement.
(iii) The existing works of the literature failed to consider the predominance of the neighboring neurons during the detection process that classifies malicious traffic from normal traffic.

3. Proposed RMPSOM enforced DDoS attack prevention mechanism

This proposed RMPSOM is an attempt for enhanced prevention of DDoS attacks in the cloud space facilitated through the investigation of the data traffic flow based on periodic monitoring achieved by the SDN control plane. The SDN-based DDoS prevention is determined to be effective since they are potential in estimating the deviation between the normal data traffic and malicious data traffic. This proposed RMPSOM uses the benefits of Rival Penalized SOM which is improved phenomenally from the traditional SOM approach by resolving the issues of decreasing function and learning rate selection in DDoS prevention. The nomenclature of symbols and their definitions used in this proposed RMPSOM are tabulated in Table 1.

In this proposed RMPSOM, the neurons are employed in the process of estimating the Euclidean distance between the actual data traffic with the expected data traffic in order to prevent DDoS attacks in the cloud space. On the entire SOM-based neuron map $r \times s$, the process of investigation starts with the random selection of input $f(t)$ derived from the data flow traffic. Initially, the neurons of the RMPSOM are assigned with a weight vector $p_i = \{p_{i1}, p_{i2}, \ldots, p_{iD}\}$ such that the dimensions of the weight and the randomly selected input are the same. The core objective of this proposed RMPSOM is to focus on the neuron whose weight

Table 1
Nomenclature of symbols and its definition used in RMPSOM.

Nomenclature	Meaning
$obj_{(val)}$	Objective function of the proposed RMPSOM
$f(t)$	Random selection of input
p_i	Weight vector
$N_{k,i}(t)$	Neighborhood kernel
$\beta(t)$ and $\kappa(t)$	Learning factors
T_P	Period of training
$Farthest(Succ(obj_{(val)}))$	Farthest proximity neurons
$Nearest(Succ(obj_{(val)}))$	Nearest proximity neurons
$\alpha_{(p,q)}$	Learning factor of the closest neuron
$Rank_{(i)}$	Ranking of neurons based on Euclidean distance
$\|y_k - y_i\|^2$	The formula used in estimating the Euclidean distance
η_i	Relative successive neuron
λ_i	Date rate
q	Close proximity neuron
$C_{d(p,q)}$	Closest distance of the near located neuron
$N_{k,q}(t)$	Weight of the close proximity neuron 'rival neuron' and its closest neighborhood neurons

vector is very close to the considered input vector evaluated in terms of Euclidean Distance. Then, two potential variables such as step and epoch variable are assigned to 1 when the weight vectors are randomly initialized. The core objective of this proposed RMPSOM is iterated until the stop condition is not satisfied based on the constraint derived from Eq. (1)

$$obj_{(val)} = \arg(\underset{t\le i\le \min}{Min}\{\|p_i(t) - f(t)\|\}) \tag{1}$$

Then, the weights and their associated neighbors are updated based on Eqs. (2) and (3)

$$p_i(t+1) = p_i(t) + N_{k,i}(t)[f(t) - p_i(t)] \tag{2}$$

and

$$N_{k,i}(t) = \beta(t) * (-\frac{\|y_k - y_i\|}{2\kappa^2(t)}) \tag{3}$$

This neighborhood kernel represented in Eq. (3) is selected based on a Gaussian function defined in [27]. This process of updating weights and related neighbors is facilitated with increased time and epochs until the epoch terminates or the mapping converges to an optimal point. Further, the potential learning factors such as $\beta(t)$ and $\kappa(t)$ decrease monotonically based on Eqs. (4) and (5)

$$\beta(t) = \beta(0) * (\frac{\beta(T_p)}{\beta(0)})^{\frac{\tau}{T_P}} \tag{4}$$

$$K(t) = K(0) * \left(\frac{K(T_p)}{K(0)}\right)^{\frac{\tau}{T_P}} \tag{5}$$

where T_P is the period of training, which is used in the process of updating weights and estimating neighborhood value in the utilized RMPSOM. However, the selection of accurate and monotonically decreasing function decreases the potential of the utilized RMPSOM mechanism. Thus, the proposed RMPSOM enforced DDoS Attack Prevention Mechanism utilizes the constant learning rate for training the neurons of SOM towards malicious traffic detection. This utilization of the constant learning rate aids in preserving the topology in order to minimize the degree of quantization error and maximum utilization of the neurons. In this constant learning rate-based RMPSOM mechanism, the nearest and farthest proximity neurons in the close neighborhood of the successor neuron are initially computed based on Eqs. (6) and (7) respectively.

$$Farthest(Succ(obj_{(val)})) = \arg(\underset{t\le i\le \min}{Max}\{\|p_i(t) - f(t)\|\}) \tag{6}$$

$$Nearest(Succ(obj_{(val)})) = \arg(\underset{t\le i\le \min}{Min}\{\|p_i(t) - f(t)\|\}) \tag{7}$$

Then, a unique rank is assigned to each of the neurons based on the distance estimated from the input considered for investigation. The unique rank of 0 is assigned to the optimal successor neuron if it is very close to the neighborhood of the input vector considered for analysis. Otherwise, the value of the optimal successor neuron is incremented monotonically in increments of 1 depending on the proximity of its location to the input vector considered for investigation.

Further, the weights of the successor neuron and their closest neighborhood neurons are updated based on Eqs. (8) and (9)

$$N_{k,i}(t) = \beta(t) * (1 - \eta_i) * \exp(-\frac{\alpha_{(p,q)}}{2\kappa^2(t)}) \tag{8}$$

$$\alpha_{(p,q)} = Rank_{(i)} + (\|y_k - y_i\|^2 + C_{d(p,q)}) \tag{9}$$

In this context, the value of the relative successive neuron η_i is computed based on Eq. (10) such that the weights of the successor neuron and their closest neighborhood neurons are determined in a reactive manner. This reactive estimation of weights aids in the better categorization of traffic data flows into normal and malicious based on the computation of the rate of data (λ_i) forwarded from the source to the destination in the cloud environment. Moreover, the value of $(1 - \eta_i)$ must lie between 0 and 1.

$$\eta_i = \frac{\lambda_i}{\sum_{i=1}^{k}\lambda_i} \tag{10}$$

In addition, the weight of the close proximity neuron 'q' (rival neuron) and its closest neighborhood neurons are computed by modifying Eqs. (2) and (3) into Eqs. (11) and (12) respectively.

$$p_i(t+1) = p_i(t) + N_{k,i}(t)[f(t) - p_q(t)] \tag{11}$$

and

$$N_{k,q}(t) = \beta(t) * (1 - \eta_i) * \exp(-\frac{\alpha_{(p,q)}}{2\kappa^2(t)}) \tag{12}$$

where, $\alpha_{(p,q)}$ is the learning factor of the closest neuron determined based on Eq. (13)

$$\alpha_{(p,q)} = \left\|(p_q(t) - f(t))\right\|^2 + C_{d(p,q)} \tag{13}$$

This process of updating weights and related neighbors is also enabled until the epoch terminates or the mapping converges to an optimal point. However, the second successive neuron (rival neuron) cannot be considered as the farthest possible proximity neurons since it violates the intrinsic characteristics of Self Organizing Maps (SOM). The learning factor $\alpha_{(p,q)}$ is considered to be kept constant in order to ensure better accuracy in the discrimination process of the data traffic flow into normal and malicious. Thus, the proposed RMPSOM-SDNDM scheme is adaptive and capable of selecting various numbers of rivals that closely possess similar features of the successor neuron for penalizing their associated models. The penalization in the associated models of rival neurons is imposed only over the real vector parameters whose dimensions are very similar to the considered input vector. The constant learning rate enabled in the proposed RMPSOM-SDNDM scheme prevents or eliminates the possibility of selecting the inessential learning rate function that monotonically decreases without converging to an optimal detection.

4. Simulation results and investigation

In this section, the role of the proposed RMPSOM-SDNDM in the effective and efficient prevention of DDoS attacks on the cloud environment is investigated using the test cases that are uniquely designed with realistic and trustworthy key features

Table 2
RMPSOM-SDNDM scheme-Predicted flow count for testing and training.

Category of DDoS Attack	Flow count used for the testing process	Flow count used for the training process
Flooding attack using TCP SYN packets	157812	6324
100 bytes packet size-based UDP flooding attack	52278	2819
200 bytes packet size-based UDP flooding attack	337896	–
400 bytes packet size-based UDP flooding attack	41067	4251
800 bytes packet size-based UDP flooding attack	128792	–
60 bytes packet size-based ICMP flooding attack	59213	–
1024 bytes packet size-based ICMP flooding attack	57235	5332

specified in [28–30]. The potential of the proposed RMPSOM-SDNDM is compared with the baseline DDoS attack prevention techniques such as FSOM-SDNDM, BF-DCFM, FRESCODM, and TRW-FLIBDM. The benchmarked schemes of FSOM-SDNDM, BF-DCFM, FRESCODM, and TRW-FLIBDM are chosen for investigation because they are determined to be the existing novel schemes that motivate the requirement of the fuzzy neural network in the rapid and reliable prevention of the DDoS attacks in the cloud computing environment. These benchmarked approaches are adaptive and dynamic in exploring and exploiting the possibilities involved in the process of training and testing that helps in the potential classification of the data traffic flows into normal and malicious data traffic. These baseline DDoS attacks prevention approaches have also potential in using Self Organizing Maps for accuracy estimation and derivation of training rules that motivate towards the distinct categorization and prevention of unwanted data traffic before exhausting the scarce resources of the cloud environment [31].

This comparative investigation of RMPSOM-SDNDM with the compared FSOM-SDNDM, BF-DCFM, FRESCODM, and TRW-FLIBDM schemes is facilitated using five influential traffic flows characteristic such as Average Time incurred Per Flow (ATPF), Percentage of Average Flow Pairs (PAFP), Growth Rate Per Flows (GRPF), Average Byte Per Flow Count (ABPFC) and Average packet per flow count (APPFC) since they are considered as the influential factors that need to be investigated for SDN-based DDoS attack prevention mechanism [31]. In this investigative process, the aforementioned traffic flows characteristics are collected through the incorporation of the flow aggregation module embedded in the utilized NOX related network. These aggregated traffic flow features are explored by the classifier module of NOX in order to enable the activity of traffic flow analysis, such that illegitimate data flows are effectively detected through the implemented RMPSOM-SDNDM scheme.

In this investigative process of the proposed RMPSOM-SDNDM scheme, different categories of malicious and legitimate traffic features are integrated together for achieving predominant testing. The legitimate data traffic generated and utilized in the process of testing comprises 80% of TCP packets, 10% of ICMP packets, and 10% of UDP packets. The testing data and training data traffic parameters are similar in order to investigate the potential of the proposed RMPSOM-SDNDM scheme. FTP connections are established for collecting and investigating 80% of TCP packets since they portray the continuous process of data dissemination maintained between the server and the client in the cloud computing environment. The remaining 10% of ICMP packets and 10% of UDP packets are gathered and analyzed using the establishment and maintenance of Telnet connections. Telnet connections are mainly used for generating and disseminating a reduced amount of data packets with maximum inter-arrival time ensured between them. In this investigation of the proposed RMPSOM-SDNDM scheme, the Stacheldraht tool is used for generating and analyzing data traffic considered for detecting DDoS attacks in the cloud environment. The predicted number of flows that are utilized for the training and testing process of the proposed RMPSOM-SDNDM scheme under the impact of diversified categories of DDoS attacks are listed in Table 2.

The experimental emulation conducted during the process of testing and training of the proposed RMPSOM-SDNDM scheme is facilitated with the help of the server, which is configured using 16 GB RAM memory capability enhanced by Intel Quad-Core Xeon processor. In this experimental investigation of the proposed RMPSOM-SDNDM scheme, the NOX oriented network script is updated with the aid of the wire filter entity such that significant parameters such as bandwidth and delay of 1 Gbps and 20 ms are maintained for sustaining the link existing between the networks [20]. In this experimental investigation of the proposed RMPSOM-SDNDM scheme, approximately 107 500 flows are initiated during the process of training with the maximum of 48 000 flows and 61 000 flows monitored and evaluated at the influence of trustworthy data traffic and in between the time of generating malicious data traffic.

Initially, Fig. 1 unveils the comprehensive attacker source topology with various attacker sources that are responsible for introducing a DDoS attack into the SDN-based cloud computing environment. In this attacker source topology, Attacker 1 introduces TCP, UDP, or ICMP packets for introducing the flooding-based DDoS attacks. Likewise, Attacker 2 uses the Legitimate IP packets for compromising the network. Further, Attacker 3 uses the Botnets for facilitating malicious behavior into the network. In addition, Attacker 4 is responsible for introducing malicious data traffic network into the SDN-based network using DNS or IP spoofing. The SDN included in the network topology is mainly for enhancing the degree of manageability, scalability, Adaptivity, and controllability. Fig. 2 exemplars the test-bed topology incorporated in the SDN-based cloud environment used for implementing the proposed RMPSOM-SDNDM scheme. The Virtual Router Firewall (VRF) present in the considered testbed is responsible for connecting the internet with the physical infrastructure of the SDN-based cloud. The VRF present in this test-bed topology is capable of permitting HTTP and HTTPs protocols based on the utilization of two load balancers LB1 and LB2. These LB1 and LB2 load balancers are embedded in the application servers that are inherently and potentially hosted in the VMware for effective processing and detection.

To be specific, Load balancer LB1 is mainly utilized for balancing the number of HTTP and HTTPs connections that aids in connecting the internet and the web servers residing in the multiple VM1, VM2, and VM3 entities that are in turn connected to the main VMware virtual machine. Load balancer LB2 is responsible for connecting three database clusters such as C1, C2, and C3 for ensuring direct interaction with the core database. In addition, the storage area network is connected with the VMware virtual machine infrastructure-based on the iSCSI (Internet Small Computer Systems Interface) protocol.

The experiments conducted for investigating the performance of the proposed RMPSOM-SDNDM scheme are three folded. First, the significance of the proposed RMPSOM-SDNDM scheme is analyzed using percentage accuracy in detection with the percentage increase in the False Positive rate by increasing the data

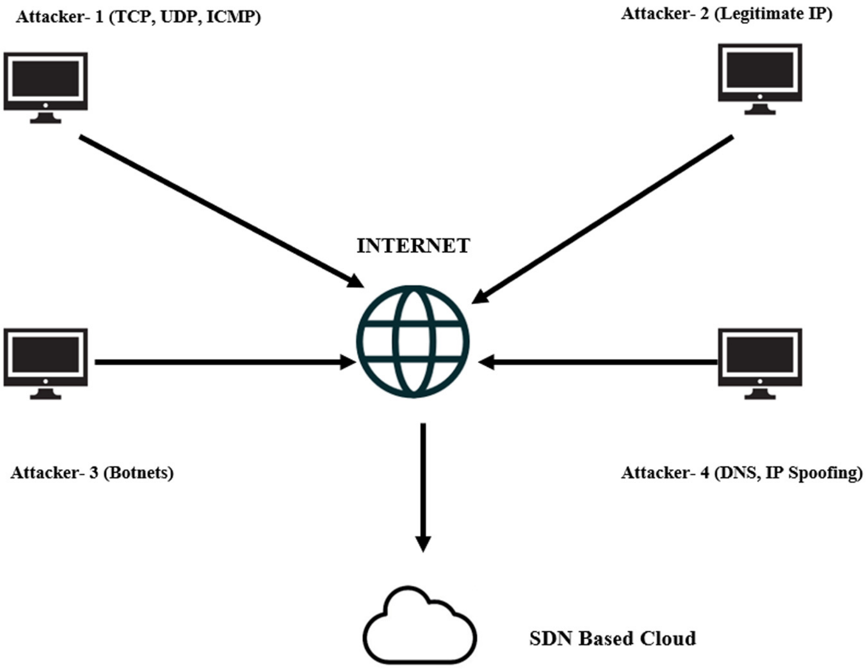
Attacker- 1 (TCP, UDP, ICMP)
Attacker- 2 (Legitimate IP)
INTERNET
Attacker- 3 (Botnets)
Attacker- 4 (DNS, IP Spoofing)
SDN Based Cloud

Fig. 1. Comprehensive Attacker Source Topology utilized for implementing the proposed RMPSOM-SDNDM scheme.

rates from 100 Mbps to 500 Mbps varied in increments of 100. Further, the potential of the proposed RMPSOM-SDNDM scheme is quantified using False Negative rate, True Positive rate, and True Negative rate evaluated under a different increase in data rates from 100 Mbps to 500 Mbps varied in increments of 50. In addition, the investigation of the proposed RMPSOM-SDNDM scheme is facilitated using True Positive rate by varying the data rates from 50 Mbps to 500 Mbps with the False Positive rate varying from 15%, 30%, and 45% respectively.

Initially, Figs. 3–7 highlight the significance of the proposed RMPSOM-SDNDM scheme using percentage accuracy in detection by varying the percentage of the False Positive rate from 0% to 75% in increments of 5% under the influence of 100 Mbps, 200 Mbps, 300 Mbps, 400 Mbps and 500 Mbps data rate respectively. Fig. 3 emphasizes that the percentage increase in Detection Accuracy of the proposed RMPSOM-SDNDM scheme under 100 Mbps data rate is determined to be 17%–21% better when compared to FSOM-SDNDM, 12%–15% superior to BF-DCFM, FRESCODM, and 9%–13% excellent than TRW-FLIBDM schemes. Similarly, Fig. 4 depicts that the percentage increase in Detection Accuracy of the proposed RMPSOM-SDNDM scheme under 200 Mbps data rate is determined to be 19%–23% better when compared to FSOM-SDNDM, 14%–17% superior to BF-DCFM, FRESCODM, and 11%–14% excellent than TRW-FLIBDM schemes.

Further, Fig. 5 exemplars that the percentage increase in Detection Accuracy of the proposed RMPSOM-SDNDM scheme under 200 Mbps data rate is determined to be 20%–24% better when compared to FSOM-SDNDM, 15%–19% superior to BF-DCFM, FRESCODM, and 13%–16% excellent than TRW-FLIBDM schemes. Furthermore, Fig. 6 depicts that the percentage increase in Detection Accuracy of the proposed RMPSOM-SDNDM scheme under 200 Mbps data rate is determined to be 22%–25% better when compared to FSOM-SDNDM, 16%–18% superior to BF-DCFM, FRESCODM, and 14%–16% excellent than TRW-FLIBDM schemes. In addition, Fig. 7 quantifies that the percentage increase in Detection Accuracy of the proposed RMPSOM-SDNDM scheme under 200 Mbps data rate is determined to be 24%–27% better when compared to FSOM-SDNDM, 19%–21% superior to BF-DCFM, FRESCODM, and 15%–18% excellent than TRW-FLIBDM schemes. From this investigation, it is very clear that the Detection Accuracy of the proposed RMPSOM-SDNDM scheme is improved on par with the baseline DDoS mitigation schemes even under increasing variation in the data rate. This predominant enhancement in Detection Accuracy is mainly due to the incorporation of the constant learning rate that aided in preserving the topology for minimizing the degree of quantization error and maximum utilization of the neurons. This quantifiable improvement in the Detection Accuracy is also facilitated by the proposed RMPSOM-SDNDM scheme through the utilized process of updating weights

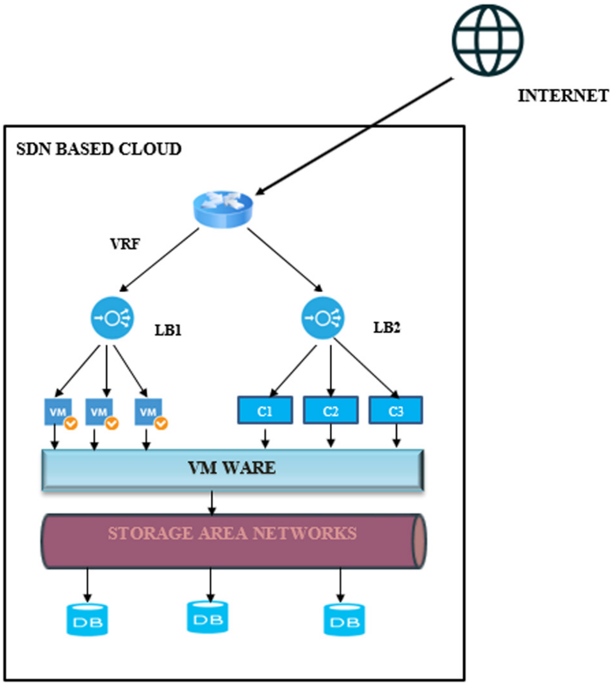

Fig. 2. The test-bed topology incorporated in the SDB-based cloud environment for implementing the proposed RMPSOM-SDNDM scheme.

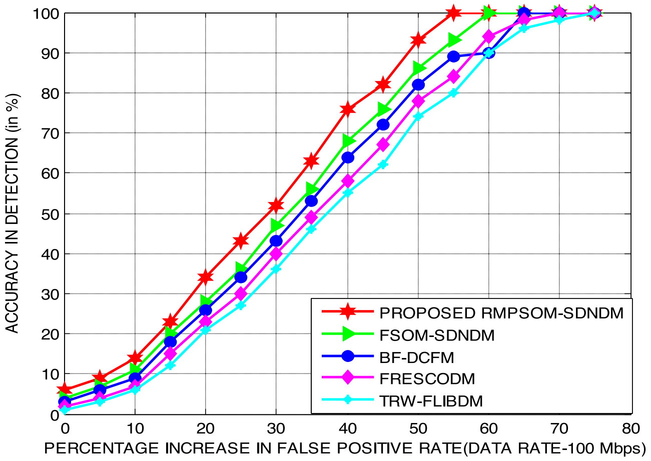

Fig. 3. Proposed RMPSOM-Detection Accuracy-varying False Positiveness (100 Mbps).

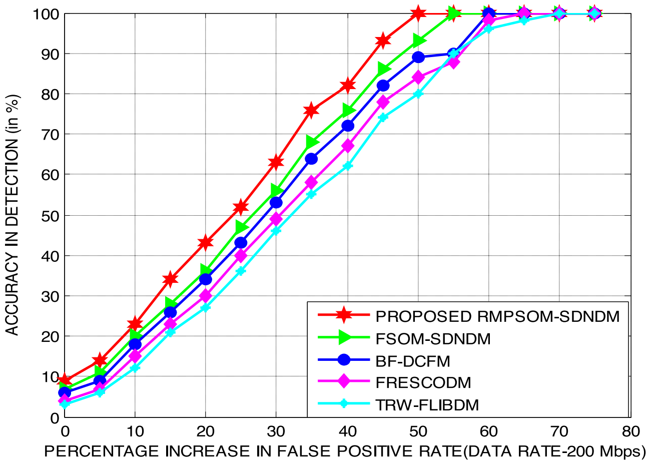

Fig. 4. Proposed RMPSOM-Detection Accuracy-varying False Positiveness (200 Mbps).

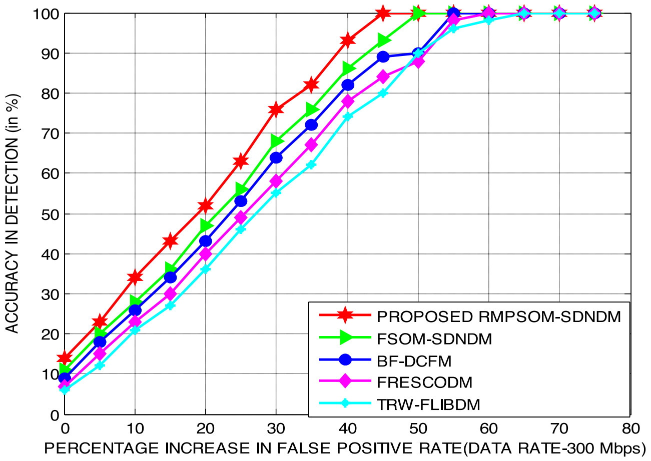

Fig. 5. Proposed RMPSOM-Detection Accuracy-varying False Positiveness (300 Mbps).

and related neighbors, which are adaptively improved to periodic increase in time and epochs until the epoch terminates or the mapping converges to an optimal point.

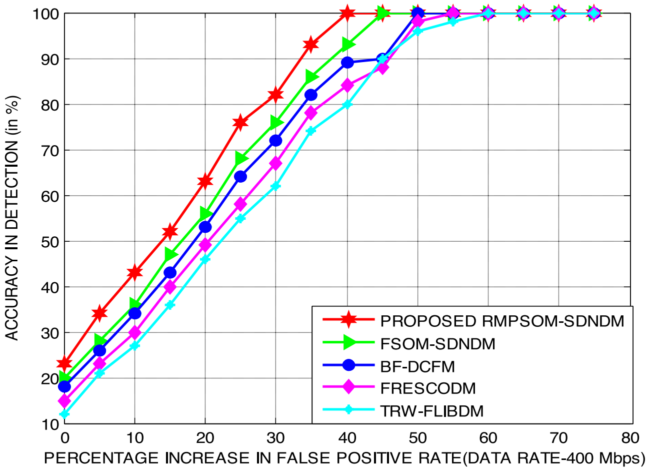

Fig. 6. Proposed RMPSOM-Detection Accuracy-varying False Positiveness (400 Mbps).

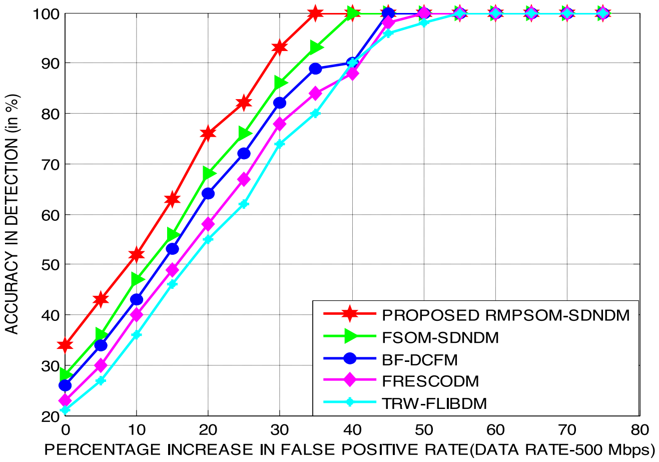

Fig. 7. Proposed RMPSOM-Detection Accuracy-varying False Positiveness (500 Mbps).

In this second process of investigation, Figs. 8–10 highlight the predominance of the proposed RMPSOM-SDNDM scheme in terms of the percentage decrease in False Negative rate, the percentage increase in True Positive rate and percentage increase in True Negative rate evaluated under the impact of varying data rates. Fig. 8 confirms that the percentage decrease in the False Negative rate of the proposed RMPSOM-SDNDM scheme is mainly due to the utilization of the learning rate, which is kept constant independent of the flow count monitored for analyzing DDoS attacks in the cloud environment. Thus, the proposed RMPSOM-SDNDM scheme reduced the False Negative rate on an average by 10%, 12%, 15%, and 18%, on par with the compared FSOM-SDNDM, BF-DCFM, FRESCODM, and TRW-FLIBDM schemes. Figs. 9 and 10 inferred that the True Positive rate and True Negative rate are increased by the proposed RMPSOM-SDNDM scheme since they are capable of discriminating the traffic flows into normal and malicious based on the assignment of unique rank to each neuron through the estimated distance determined from the input data traffic flows. Hence, the proposed RMPSOM-SDNDM scheme increases the True Positive rate on an average by 13%, 16%, 18% and 21% on par with the compared FSOM-SDNDM, BF-DCFM, FRESCODM, and TRW-FLIBDM schemes. In addition, the proposed RMPSOM-SDNDM scheme increased the True Negative rate on an average by 7%, 10%, 13%, and 15% on par with the compared FSOM-SDNDM, BF-DCFM, FRESCODM, and TRW-FLIBDM schemes.

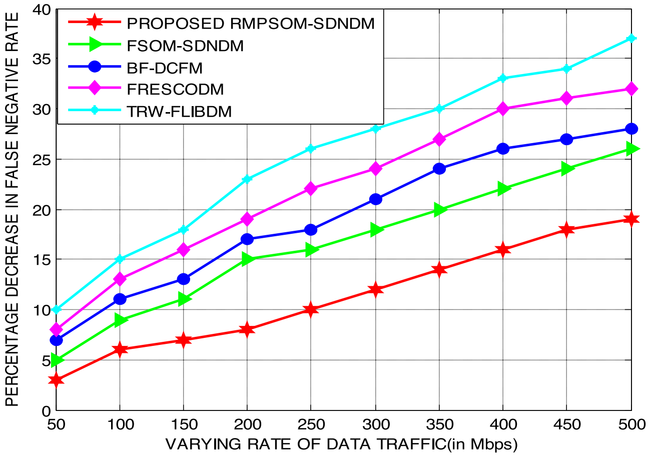

Fig. 8. Proposed RMPSOM-percentage increase in False Negative.

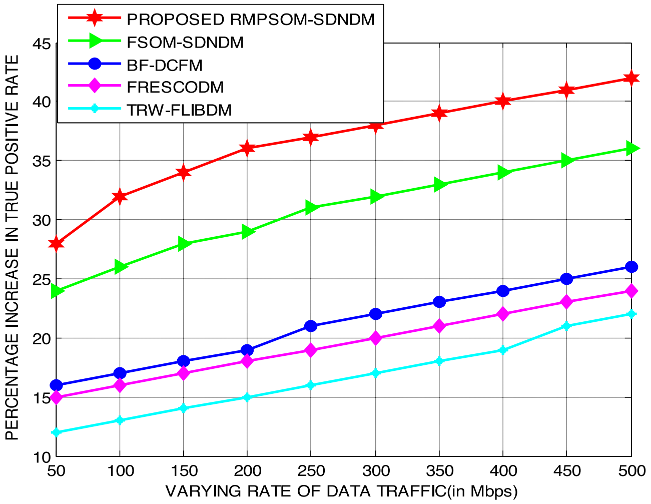

Fig. 9. Proposed RMPSOM-percentage increase in True Positive.

Finally, the proposed RMPSOM-SDNDM scheme is evaluated using True Positive rate by varying the data rates from 50 Mbps to 500 Mbps in increments of 50 Mbps with the False Positive rate varying from 15%, 30%, and 45% respectively. Figs. 11, 12, and 13 unveil the True Positive rate of the proposed RMPSOM-SDNDM scheme quantified under varying intensities of 15%, 30%, and 45% in False Positive rates. Fig. 11 proved that the True Positive rate of the proposed RMPSOM-SDNDM scheme under 15% intensity of False Positive rate is maximum up to a level of 0.92 which is nearly 7%, 9%, 12%, and 15% greater than the benchmarked FSOM-SDNDM, BF-DCFM, FRESCODM, and TRW-FLIBDM schemes. Similarly, Fig. 12 ensured that the True Positive rate of the proposed RMPSOM-SDNDM scheme under 30% intensity of False Positive rate is maximum up to a level of 0.89 which is approximately 6%, 8%, 10%, and 13% excellent than the baseline FSOM-SDNDM, BF-DCFM, FRESCODM, and TRW-FLIBDM schemes considered for analysis.

In addition, Fig. 13 clarified that the True Positive rate of the proposed RMPSOM-SDNDM scheme under 45% intensity of False Positive rate is maximum up to a level of 0.86 which is approximately 5%, 9%, 12%, and 15% predominant to the compared FSOM-SDNDM, BF-DCFM, FRESCODM and TRW-FLIBDM schemes considered for investigation.

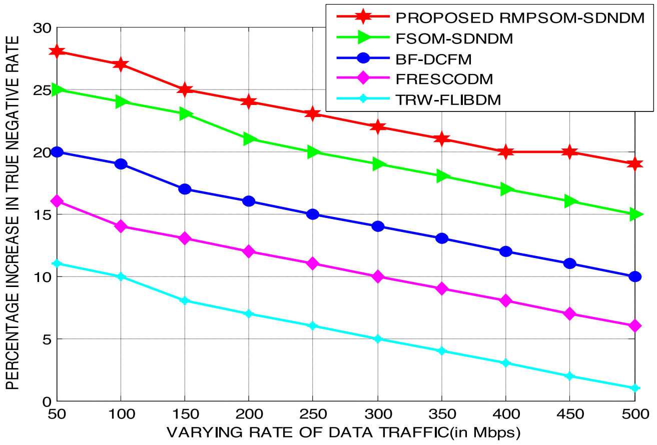

Fig. 10. Proposed RMPSOM-percentage increase in True Negative.

Tables 3–5 are presented for portraying the predominant results of the proposed RMPSOM-SDNDM scheme over the compared FSOM-SDNDM, BF-DCFM, FRESCODM and TRW-FLIBDM schemes using Precision, Recall, and Optimality rate evaluated under different data rates varying from 100 Mbps to 500 Mbps. This investigation is essential because the techniques contributed to detecting and preventing DDoS attacks in cloud environment need to be more precise with potent recall value and optimality rate [31].

The results highlighted in Tables 3, 4, and 5 proved that the Precision, Recall, and Optimality rate of the proposed RMPSOM-SDNDM scheme are enhanced on an average by 10%, 8% and 9% compared to the baseline FSOM-SDNDM, BF-DCFM, FRESCODM and TRW-FLIBDM schemes used for analysis.

The reasons behind the potential performance of the proposed RMPSOM-SDNDM scheme over the benchmarked schemes are listed as follows.

(i) The use of rival penalized SOM minimized the failure rate of the classifier that segregated malicious data traffic and normal data traffic flows.
(ii) It attained a better classification function despite the utilization of a monotonically decreasing function that generally leads to poor convergence.
(iii) The inclusion of constant learning rate increased the probability of selecting an accurate and reliable learning rate function that increases the accuracy degree to the expected level.

5. Conclusions

The proposed RMPSOM-SDNDM scheme was contributed for SDN-based DDoS attack prevention scheme in order to attain rapid and accurate detection with the benefits of rival penalized SOM and constant learning rate. It included the merits of the constant learning rate that opened wide the probability of selecting an accurate and reliable learning rate function. This learning rate used in RMPSOM included a monotonically decreasing function that attained robust performance by converging to an optimal point of detection. It categorized data flows into normal and malicious based on the weight of the neuron whose weight vector is very close to the Euclidean distance of the considered input vector. The simulation results of the proposed RMPSOM-SDNDM scheme proved that the Detection Accuracy under varying data rates from 100 Mbps to 500 Mbps is improved over the benchmarked approaches by a significant mean margin of 18%. The

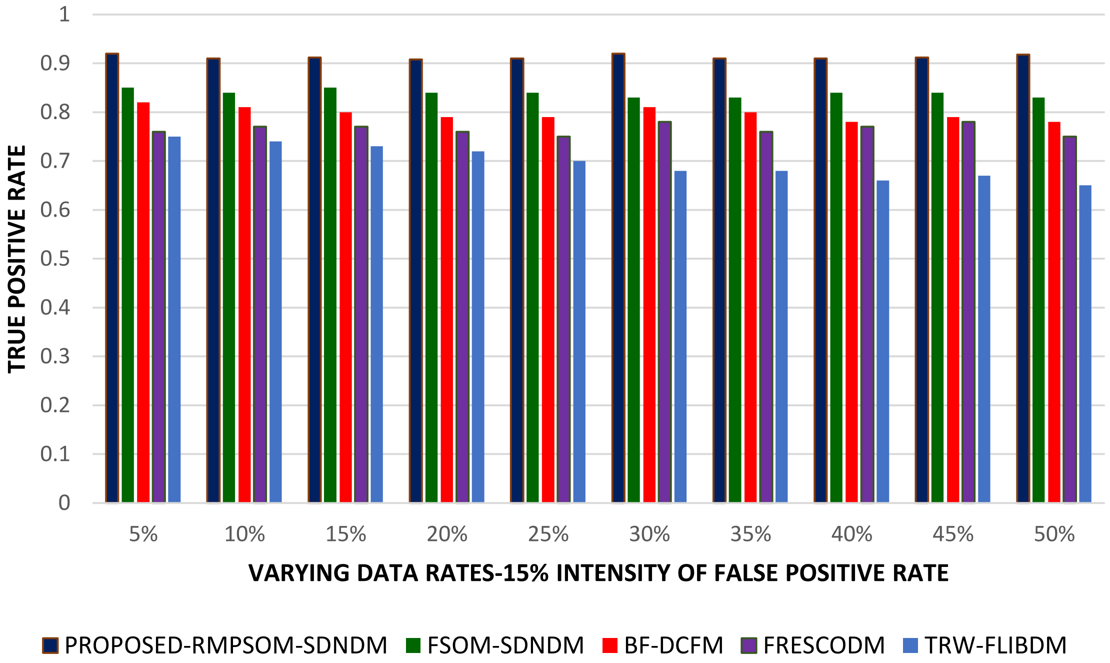

Fig. 11. Proposed RMPSOM-percentage increase in True Positive rate (intensity of False Positive rate—15%).

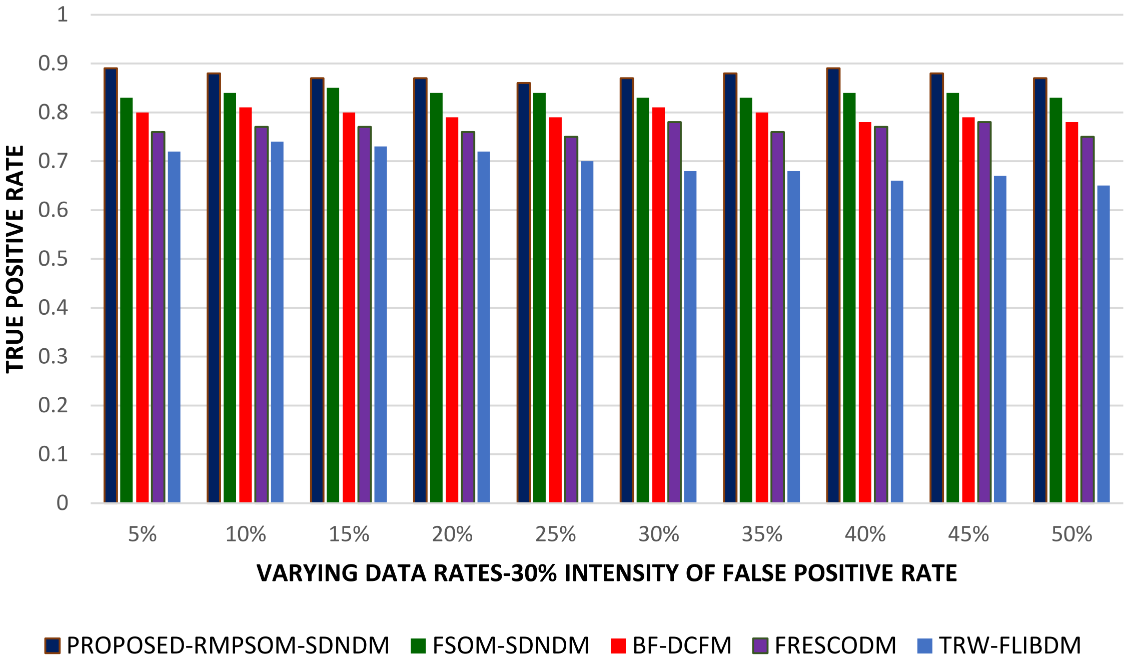

Fig. 12. Proposed RMPSOM-percentage increase in True Positive rate (intensity of False Positive rate—30%).

Table 3
Proposed RMPSOM-SDNDM evaluated using precision value.

DDoS prevention schemes	Precision Value under varying data rates				
	100 Mbps	200 Mbps	300 Mbps	400 Mbps	500 Mbps
Proposed RMPSOM-SDNDM	0.982	0.980	0.989	0.987	0.989
FSOM-SDNDM	0.967	0.963	0.956	0.965	0.968
BF-DCFM	0.945	0.949	0.952	0.954	0.958
FRESCODM	0.932	0.936	0.938	0.942	0.945
TRW-FLIBDM	0.921	0.927	0.932	0.931	0.937

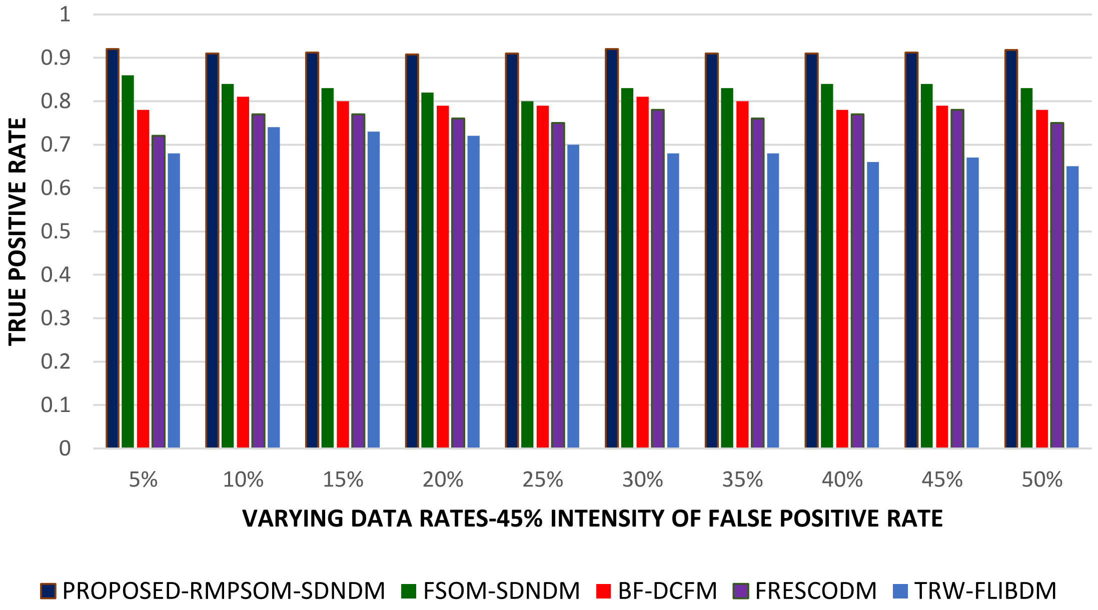

Fig. 13. Proposed RMPSOM-percentage increase in True Positive rate (intensity of False Positive rate—45%).

Table 4
Proposed RMPSOM-SDNDM evaluated using recall value.

DDoS prevention schemes	Recall Value under varying data rates				
	100 Mbps	200 Mbps	300 Mbps	400 Mbps	500 Mbps
Proposed RMPSOM-SDNDM	0.986	0.985	0.982	0.984	0.980
FSOM-SDNDM	0.953	0.952	0.951	0.948	0.941
BF-DCFM	0.945	0.939	0.931	0.928	0.924
FRESCODM	0.932	0.931	0.928	0.921	0.918
TRW-FLIBDM	0.913	0.910	0.908	0.909	0.912

Table 5
Proposed RMPSOM-SDNDM evaluated using optimality value.

DDoS prevention schemes	Optimality Value under varying data rates				
	100 Mbps	200 Mbps	300 Mbps	400 Mbps	500 Mbps
Proposed RMPSOM-SDNDM	0.976	0.974	0.972	0.970	0.965
FSOM-SDNDM	0.943	0.942	0.940	0.935	0.932
BF-DCFM	0.932	0.930	0.927	0.925	0.922
FRESCODM	0.912	0.916	0.910	0.908	0.909
TRW-FLIBDM	0.893	0.892	0.891	0.883	0.873

False Positive rate, True Positive rate, and True Negative rate of the proposed RMPSOM-SDNDM scheme are minimized on an average of 11.25% compared to the schemes considered for investigation. The results also confirmed that the Precision, Recall, and Optimality rate of the proposed RMPSOM-SDNDM scheme are enhanced on an average by 10%, 8%, and 9% compared to the baseline schemes used for analysis. In the near future, it is also planned to formulate a fuzzy TOPSIS-based DDoS attack detection scheme that explores possible parameters that could be considered in the process of mitigating its influence on the SDN network.

CRediT authorship contribution statement

Pillutla Harikrishna: Conception and design of study, Acquisition of data, Analysis and/or interpretation of data, Writing - original draft, Writing - review & editing. **A. Amuthan:** Conception and design of study, Acquisition of data, Analysis and/or interpretation of data, Writing - original draft, Writing - review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

All authors approved the version of the manuscript to be published.

References

[1] O. Osanaiye, K.R. Choo, M. Dlodlo, Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework, J. Netw. Comput. Appl. 67 (2016) 147–165.

[2] T. Karnwal, S. Thandapanii, A. Gnanasekaran, A filter tree approach to protect cloud computing against XML DDoS and HTTP DDoS attack, Adv. Intell. Syst. Comput. 1 (1) (2013) 459–469.

[3] T. Nathiya, Reducing DDOS attack techniques in cloud computing network technology, Int. J. Innov. Res. Appl. Sci. Eng. 1 (1) (2017) 23.

[4] L. Ya-Dong, Study on detection algorithm of ddos attack for cloud computing, in: 2014 Fifth International Conference on Intelligent Systems Design and Engineering Applications, Vol. 1 (1) 2014, pp. 67–75.

[5] B.S. Devi, T. Subbulakshmi, DDoS attack detection and mitigation techniques in cloud computing environment, in: 2017 International Conference on Intelligent Sustainable Systems (ICISS), Vol. 1 (1) 2017, pp. 54-63.

[6] A. Amuthan, P. Harikrishna, Mean availability parameter-based DDoS detection mechanism for cloud computing environments, Wireless Commun. Netw. Internet Things 1 (1) (2018) 115–122.

[7] R. Aishwarya, S. Malliga, Intrusion detection system- An efficient way to thwart against Dos/DDos attack in the cloud environment, in: 2014 International Conference on Recent Trends in Information Technology, Vol. 1 (1) 2014, pp. 12-24.

[8] G. Somani, M.S. Gaur, D. Sanghi, M. Conti, R. Buyya, DDoS attacks in cloud computing: Issues, taxonomy, and future directions, Comput. Commun. 107 (1) (2017) 30–48.

[9] H. Toumi, B. Marzak, A. Talea, A. Eddaoui, M. Talea, Use trust management framework to achieve effective security mechanisms in cloud environment, Int. J. Interact. Multimed. Artif. Intell. 4 (3) (2017) 70.

[10] Q. Yan, F.R. Yu, Q. Gong, J. Li, Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges, IEEE Commun. Surv. Tutor. 18 (1) (2016) 602–622.

[11] S. Lee, J. Kim, S. Shin, P. Porras, V. Yegneswaran, Athena: A framework for scalable anomaly detection in software-defined networks, in: 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Vol. 1 (1) 2017 pp. 33-44.

[12] Q. Yan, F.R. Yu, Distributed denial of service attacks in software-defined networking with cloud computing, IEEE Commun. Mag. 53 (4) (2015) 52–59.

[13] H. Vaishali, B. Harish, An efficient way to prevent Dos/DDos attack in the cloud environment, Int. J. Sci. Res. 5 (3) (2016) 829–832.

[14] P. Lin, Y. Hsu, R. Hwang, Detecting and preventing DDoS attacks in SDN-based data center networks, Cloud Comput. Secur. 1 (1) (2017) 50–61.

[15] S. Lee, C. Yoon, C. Lee, S. Shin, V. Yegneswaran, P. Porras, DELTA: A security assessment framework for software-defined networks, in: Proceedings 2017 Network and Distributed System Security Symposium, Vol. 1 (1) 2017, pp. 54-65.

[16] N. Patel Zalak, Preventing cloud systems against ddos attack using hop count filter approach, Int. J. Adv. Res. Comput. Sci. 9 (2) (2018) 320–323.

[17] P. Xiao, Z. Li, H. Qi, W. Qu, H. Yu, An efficient ddos detection with bloom filter in SDN, in: 2016 IEEE Trustcom/BigDataSE/ISPA, Vol. 1, (1) 2016, pp. 45–54.

[18] S. Shin, L. Xu, S. Hong, G. Gu, Enhancing network security through software defined networking (SDN), in: 2016 25th International Conference on Computer Communication and Networks (ICCCN), Vol. 2 (1) 2016, pp. 89-97.

[19] Y. Xu, Y. Liu, DDoS attack detection under SDN context, in: IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications, Vol. 1 (1) 2016, pp. 78-89.

[20] H. Pillutla, A. Arjunan, Fuzzy self organizing maps-based DDoS mitigation mechanism for software defined networking in cloud computing, J. Ambient Intell. Humaniz. Comput. 10 (4) (2018) 1547–1559.

[21] Jie Cui, Mingjun Wang, Yonglong Luo, Hong Zhong, DDoS detection and defense mechanism based on cognitive-inspired computing in SDN, Future Gener. Comput. Syst. 97 (2019) 275–283.

[22] Myo Myint Oo, Sinchai Kamolphiwong, Thossaporn Kamolphiwong, Sangsuree Vasupongayya, Advanced support vector machine- (ASVM-) based detection for distributed denial of service (DDoS) attack on software defined networking (SDN), J. Comput. Netw. Commun. (2019) 8012568, 12.

[23] S. Badotra, S.N. Panda, SNORT based early DDoS detection system using Opendaylight and open networking operating system in software defined networking, Cluster Comput. (2020).

[24] R. Santos, D. Souza, W. Santo, A. Ribeiro, E. Moreno, Machine learning algorithms to detect DDoS attacks in SDN, Concurr. Comput. Pract. Exper. 32 (2020) e5402.

[25] M.M. Oo, S. Kamolphiwong, T. Kamolphiwong, S. Vasupongayya, Analysis of features dataset for DDoS detection by using ASVM method on software defined networking, Int. J. Netw. Dist. Comput. 2 (1) (2020) 45–57.

[26] A. Altan, R. Hacıoğlu, Model predictive control of three-axis gimbal system mounted on UAV for real-time target tracking under external disturbances, Mech. Syst. Signal Process. 138 (2020) 106548.

[27] Y. Yan, M.G. Genton, Gaussian likelihood inference on data from trans-Gaussian random fields with Matérn covariance function, Environmetrics 29 (5–6) (2017) e2458.

[28] J. Zhang, Y. Zhang, J. He, O. Jin, A robust and efficient detection model of DDoS attack for cloud services, Algorithms Archit. Parallel Process. 1 (1) (2015) 611–624.

[29] P. Xiao, W. Qu, H. Qi, Z. Li, Detecting DDoS attacks against data center with correlation analysis, Comput. Commun. 67 (1) (2015) 66–74.

[30] J. Zhang, Y. Zhang, P. Liu, J. He, A spark-based DDoS Attack Detection Model in Cloud Services, Inf. Secur. Pract. Exp. 1 (2) (2016) 48–64.

[31] X. Zhao, Study on DDoS attacks based on DPDK in cloud computing, in: 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT), Vol. 1 (2) 2017, pp. 67-74.

Pillutla Harikrishna is an Assistant Professor in the Department of Computer Science and Engineering at Rajeev Gandhi Memorial College of Engineering and Technology, Nandyal. He had received his Ph.D. (Computer Science and Engineering) in 2019 from Pondicherry University. He received his M.Tech. (Information Security) in 2010 and B.Tech. (Computer Science and Engineering) in 2008 from Pondicherry University. He has published more than 12 research papers and has presented more than 11 papers at conferences. His current area of research includes Cloud Computing, Network Security and Information Security.

A. Amuthan is a Professor in Pondicherry Engineering College, Puducherry. He received his Ph.D. in CSE in the year 2012. He received his M.E. from Anna University in the year 2002 and B.Tech. in the year 1996. He is a member of ISTE professional body and he has published more than 30 papers in international journals and conferences. His area of interest includes information Security and Computer Networks.