The Indonesian Journal of Computer Science
www.ijcs.net
Volume 14, Issue 3, August 2025
https://doi.org/10.33022/ijcs.v14i4.4888

Enhanced Security Algorithm for Detecting Distributed Denial of Services Attacks in Cloud Computing

Coster Baloyi[1], Topside Mathonsi[2], Deon Du Plessis[3], Tshimangadzo Tshilongamulenzhe[4]
costbal@gmail.com [1], mathonsite@tut.ac.za[2], duplessisdp@tut.ac.za[3], tshilongamulenzhetm@tut.ac.za [4]
[1,2,3,4] Tshwane University of Technology

Article Information

Received : 25 May 2025
Revised : 3 Jul 2025
Accepted : 19 Jul 2025

Keywords

DDoS, Cybersecurity, Cloud Computing, RTNTAD, MATLAB

Abstract

Cloud Computing has the benefit of offering on-demand scalable services to its customers without having to invest much on hardware infrastructure, resources and software. Most private and public sectors are moving to the Cloud. As a result, Cloud Computing has become an ideal option due to its flexibility, scalability and cost efficiency. The existence of vulnerabilities in the network systems hosting Cloud have raised an opportunity for attackers to launch attacks in Cloud Computing. The intruders attack business applications such as webservers, financial servers, and other servers exploiting Distributed Denial of Service (DDoS) attacks. This paper proposed a Real-Time Network Traffic Attack Detection (RTNTAD) algorithm to detect DDoS attacks using real-time dataset to mitigate DDoS attacks. MATLAB was employed to evaluate the performance of RTNTAD. The proposed RTNTAD algorithm has achieved 99.2% detection rate, 99.5% classification of DDoS attacks, 0.9% connectivity time out and less than 18% false positive. These outcomes suggest that RTNTAD can be seamlessly integrated into existing cloud infrastructures to proactively defend against DDoS attacks, thereby reducing service disruptions and financial losses. By enabling early detection and rapid response, the algorithm contributes to enhancing trust and resilience in cloud services, an essential factor as both public and private sectors increasingly migrate to cloud computing for its scalability, cost-efficiency, and flexibility.

A. Introduction

Cloud Computing is the imminent forthcoming of computing segment and it is assumed to be the coming generation of Internet. Cloud Computing has the benefit of centralizing different computer services in one server [1], [2]. Applications and data hosted on premise are being removed from PCs local servers and desktops computers and migrated to the private Cloud. Cloud Computing has resolved many issues regarding time, effort and costs by providing services in a reasonable amount and with less effort [3]. This comes with the benefit of increasing volume and technological capabilities off premise [4]. Furthermore, Cloud Computing offers diverse categories of services to its users commonly known as Infrastructure as a Service (IaaS), Platform as a Services (PaaS), and Software as a Services (SaaS) [5].

There are different attacks that causes severe disruption to data stored in the Cloud such as Structured Query Language (SQL) injection attack, Denial of Service (DoS) attack, Distributed Denial of Service (DDoS), and Cross-site scripting (XSS), but several authors highlighted DDoS attack as the most problematic attack due to its ability to deplete resources within network system [6], [7], [8], [9]. DDoS attacks can be prepared to send simultaneous attacks to multiple systems from one source by sending millions of packets to slow down the network services [9]. DDoS attacks can attack on a network, on an application, and moreover on the websites or online services to disrupt availability of services. The victims that are affected by these attacks are mainly service providers, large companies, commercial services and government organizations are also targeted [9].

The review of literature has indicated that other researchers have designed and implemented different security algorithms in order to detect User Datagram Protocol (UDP) and Transmission Control Protocol Synchronize (TCP SYN) flooding attacks in Cloud Computing environment [10], [11]. However, according to Awan et al. [12], the existing security algorithms for monitoring and detecting DDoS attacks such as Multi-Layer Perception (MLP), Random Forest (RF) algorithm, Naive Bayes and Data Mining algorithm are still challenged by classifying malicious attacks from normal network traffic when a large amount of network traffic is being transmitted at a high speed. Thus, these security algorithms suffer from high false positives due to poor detection accuracy. This is because these algorithms do not utilize real-time dataset in order to detect DDoS attacks in the network system. In addition, these security algorithms require more time to examine every packet being transmitted due to their computational complexity which lead to poor Quality of Services (QoS) in Cloud Computing.

In section one the research study offered a detailed background of the DDoS attacks and the impact they cause in the organizational network system. The section further highlighted the problem that the research study has found and what it intends to achieve. In section two, the research study presents a review of literature on numerous forms of DDoS attacks available in the network. In section three the research study focuses on the System Architecture and Design, giving the details of how the research study was carried out to achieve the desired results. In section four this research study presented the proposed RTNTAD algorithm. The RTNTAD algorithm is using the real time dataset to detect DDoS attacks. In section five, the research study presented the system implementation details. In section six, the

research presented the testing and results. In section seven, the research offered the conclusions and the future work and lastly the acknowledgement in section eight.

B. Related Works

In order to ensure that DDoS attacks in the network system are detected effectively and accurately with less false positives a number of studies were proposed in the past years.

Zekri et al. [13] proposed an IDS Signature-based scheme that utilized C4.5 algorithm in order to improve the detection accuracy of DDoS attacks. The C4.5 algorithm and signature detection scheme were used to create a decision tree in order to provide effective and automatic detection of DDoS attacks. Due to constrain in resources, an OpenStack Juno simulation tool was used to simulate the results in a virtualized environment where a virtual LAN and a list of VMs were utilized. The simulation results showed that the C4.5 algorithm improves the detection accuracy of 98.8% in 0.58 second when compared to Naïve Bayesian which the detection accuracy was 91.4% in 1.25 second. The limitation of the scheme is that it did not use the real-time dataset, thus it is unable to detect unknown attacks in Cloud Computing.

Awan et al. [12] proposed a Machine Learning (ML) approach that involved two mechanisms namely: MLP and RF in order to detect the DDoS attacks in real time. They utilized the big data model Spark and Scikit ML for evaluating the performance on Google Colab library. They used Databricks Community Editions in order to evaluate their solution. Their study included Apache Spark tool which is a big data tool to train and test the time measured per minutes. Their proposed solution achieved 99.5% detection accuracy thus their solution could detect attacks real-time within few milliseconds. The real-time dataset utilised is called Dos Dataset which operate in the application layer. The limitation of their scheme is that it is unable to examine every packet when a large amount of traffic is being transmitted at a high speed in Cloud Computing.

Wang et al. [14] proposed an IDS anomaly-based scheme solution that depend on the DDoS attack mitigation architecture utilizing software-defined networking (DaMask) in order to address challenges of security in Cloud Computing and demonstrate that DDoS attack defense can be much more efficient and effective. DaMask comprises of three layers, the network switches, controller and application which enhance defence mechanism again DDoS attacks. Their study shows that the successful implementation of a software-defined network (SDN) scheme enables enterprises to defend against DDoS attacks. Their study added the use of the Snort to enhance performance which provided a positive online test process. The cloud service Amazon EC2 was used for simulation. The results of the study showed that the scheme works well under new challenges on the network while reducing computation and communication overhead. The concern with this approach is that the study did not use the real-time dataset to deal with both new and old attacks effectively to avoid further DDoS attacks in a complex network environment.

Abbas & Almhanna [15] proposed an IDS Anomaly-based scheme that utilized Data Mining algorithm in order to detect DDoS attacks in the network system. The scheme was divided in to four segments, the first segment is pre-processing, the second segment is the anomaly detection model where classification of classes of

features in training step is done using Naïve Bayes (NB) algorithm and extraction of data patterns is done using Random Forest (RF) algorithm to compare the results. In the third segment the results were tested utilizing the trained dataset. The fourth segment offered the collection of system performance evaluation metrics such as detection rate, accuracy, precision and false alarm. Their study utilized the MIX dataset and further combined PORTMAP and LDAP datasets. Their accuracy in detection was 99.98% with the detection rate of 100%, and no false alarms were detected. The limitation with their scheme is that the dataset used is not real-time and that the proposed RF and NB system was not online.

Bhaya & Manaa [16] proposed an unsupervised data mining scheme called Clustering Using Representation (CURE) in order to improve the DDoS attacks detection in the network system as intrusion detection system. Their study utilized the framework of entropy for windowing the packets as they come and data mining scheme using CURE to detect DDoS attacks. Their study utilized the CAIDA2007, CAIDA2008 and DARPA2000 datasets. Their results showed 96.29% detection rate, zero per cent false positive and more than 99% accuracy. The limitation to this approach is that it requires more time to training the datasets.

Zhang et al. [17] proposed a Distributed Random Forest Based on Spark (DRFBS) technique in order to handle high-speed traffic data in real time in a network system. The DRFBS technique comprises of three segments namely: a segment that captures data through NetFlow, a data pre-processing segment and an intrusion detection based on classification. Their study was achieved by comparing the techniques such as Adaboost, multiclass support vector machine (MSVM), gradient boosting decision tree (GBDT) and random forest (RF) techniques. Their study utilized CICIDS2017 dataset to perform real-time detection of DDoS attacks. The simulation of their techniques was done through the kafka, Spark and logstash. Their results showed that DRFBS technique achieved 96.4% of the precision, 96.9% recall and 0.01second detection time. RF technique 97.9% of the precision, 97.6 recall and 1.10 second detection time. GBDT technique achieved 98.2% precision, 97.4 recall and 5.39 second detection time. Adaboost technique achieved 88.7% precision, 95.1 recall and 19.56 second detection time. MSVM technique achieved 94.5% of precision, 84.5 recall and 2600.36 second detection time as shown below:

Table 1. Summary of the Results of the Techniques Employed, Zhang et al. [17]

Technique	**DRFBS**	**RF**	**GBCT**	**Adaboost**	**MSVM**
Precision (%)	96.4	97.9	98.2	88.7	94.5
Recall (%)	96.6	97.6	97.8	95.1	84.5
Detection Time (s)	00.1	1.10	5.39	19.56	2600.36

Their study was relevant as it proved that their proposed approach has satisfactory accuracy and efficiency. The limitation to this approach is the probability of success (96% precision rate) for DRFBS technique which still requires enhancement.

Yin et al. [18] proposed a deep learning technique for intrusion detection utilizing recurrent neural networks (RNN-IDS) in order to explore how to model intrusion detection systems in the network system. The study utilized the NSL-KDD dataset. The training of data in the RNN-IDS model consists of two sections, namely:

Forward propagation which is used for calculating the values and back propagation which pass the outstanding data. The results showed that RNN-IDS has a good accuracy rate of 97.09% on the testing dataset and higher than the detection rate on the NSL-KDD dataset which was only 94.1%. The study has demonstrated that RNN-IDS has a good modelling capability and a high accuracy detection rate. The limitation of the study is that the detection rate on the NSL dataset is only 94.1% which still requires enhancement, and it requires more training time.

Abdulrahman & Ibrahem [19] proposed a hosted based intrusion detection technique for handling numerical data utilizing the following techniques, namely: Naïve Bayes (NB), C5.0, Support Vector Machine (SVM) and Random Forest (RF) in order to select the best technique for intrusion detection in the network system. Their study utilized the CICIDS2017 dataset with 225711 samples for training and testing. The simulation of their study was done using R studio software. Out of the four techniques evaluated, the results showed that C5.0 technique achieved 86% accuracy, 86% recall, 99% precision, 81% detection rate and 0.46% false positive. RF technique achieved 86% accuracy, 86% recall, 99% precision, 81% detection rate and 0.50 false positive. NB technique achieved 80% accuracy, 90% recall, 86% precision, 73% detection rate and 64% false positive. SVM technique achieved 80% accuracy, 92% recall, 86% precision, 73% detection rate and 75% false positive as shown below.

Table 2. Summary of the Performance Results Abdulrahman & Ibrahem [19]

Technique	**C5.0**	**RF**	**NB**	**SVM**
Accuracy (%)	86	86	79	79
Recall (%)	86	86	90	92
Precision (%)	99	99	86	84
Detection Rate (%)	81	81	73	75
False positive (%)	0.46	0.50	64	75

The 86% accuracy for both the C5.0 technique and the RF technique supersede the others with an accuracy average as shown in Table 2. The limitation to this study is that the 86% accuracy for both C5.0 and RF techniques still requires enhancement.The previous studies have not highlighted and attempted to propose a scheme that can detect DoS attacks using real-time datasets to mitigate the challenges of large amount of network traffic data transmitted in the network. The proposed algorithm has the capability of detecting DDoS attacks as soon as they enter the network. The DDoS attacks are effectively detected in real-time with low false positive and high detection rate in Cloud Computing.

C. System Architecture and Design

This paper proposed an enhanced security algorithm order to detect DDoS attacks using real-time dataset to mitigate the challenges of large amount of network traffic data transmitted in the network. The proposed algorithm has the capability of detecting DDoS attacks as soon as they enter the network. The DDoS attacks are effectively detected in real-time with low false positive and high detection rate in Cloud Computing.

The proposed Real-Time Network Traffic Attacks Detection (RTNTAD) algorithm was designed by integrating three existing algorithms namely, Adaptive Cumulative Sum (CUSUM) algorithm, the Exponentially Weighted Moving Average (EWMA) algorithm and Naïve Bayes in order to improve the detection accuracy of DDoS attacks in Cloud Computing.

The overview of the entire system design is demonstrated through the use of the flow diagram in Figure 1, which illustrates the nodes that form a typical Cloud Computing Wireless Sensor Network (WSN) are the sensor nodes and the base station. The bases station that is also referred to as the sink node, is a node that due to its role as a controlling node behaves as the interface between the sensor nodes and the slaves of the network. The sensor nodes that is also referred to as the simply node are devices which are small in nature and are capable of detecting the sounding environment.

The assumption is that there are M nodes in the network system. The sensor nodes produce sensor information and combine the information packets. The base station allots the information from the sensor nodes from time to time. There are a number of malicious nodes in the network. The assumption is that the number of malicious nodes is $x(0<x\ll m)$ in order to assess all the packets passing through the network. The DDoS attacks threatens the routing layer of the WSN. The below system architecture represent the challenges of such attacks in Cloud Computing WSN.

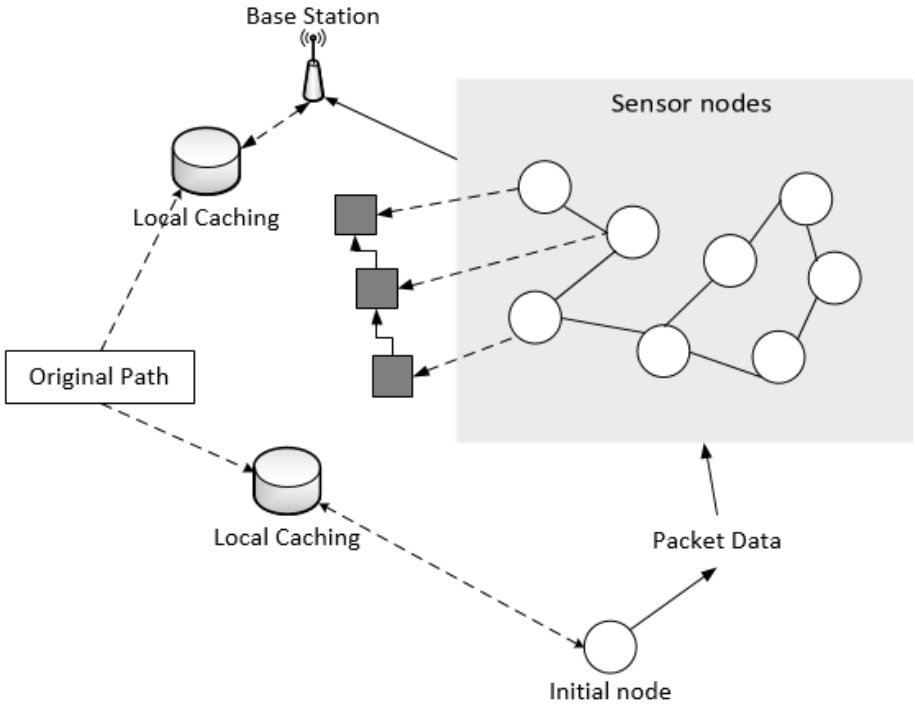

Figure 1. The proposed system architecture [20]

The architecture in Figure 1, represent the communication of data in Cloud Computing which is a method of packet data relay from the initial node to the base station [20]. In order to determine whether there was an attack or not the packet have to reach to the base station point successfully confirming that there were no

malicious nodes on the path, if not, then the packet was malicious. Then, this is therefore utilized to enhance the quality of the succeeding information packets and implement intrusion detection [20].

The assumption is that if the packet data from the initial node point successfully arrives at the base station point, therefore the route path is likely to be secured. This can be presented as follows [20]:

1. When the initial point note (N) directs to the base station (P), while N appends an empty list (M) to each packet data. When node in the sensor (I_k) collects a packet data and it is regarded as a normal node, it should add (g_k) as its identity to M.
2. The possibility is that the malicious nodes may disguise themselves by taking the same action.
3. When the packet data arrive, P extracts $M = \{g\_1, g\_2, \ldots, g\_n\}$ (here g_i refers to the identity of a relay sensor node (I_i) from the packet data and keeps it in its local caching. Here M is referred as an original path in this case.
4. P add M to a notification packet and sends the packet to N. The sensor nodes in M are used as the relay nodes.
5. When a relay sensor node (I_j) collects the warning packet, if its distinctiveness is g_j it utilizes M, then it extracts a sub route path $M\_j = \{g\_j + 1, g\_j + 2, \ldots, g\_n\}$ from M and keeps it into its local caching. (I_j) extracts its next-hop node ($I_j - 1$) with distinctiveness is $g_j - 1$ from M and forwards the packet to it.
6. On the arrival of the warning packet, N extracts M from the packet and keeps it into its local caching.

D. Proposed Real-Time Network Traffic Attacks Detection Algorithm

The RTNTAD algorithm is as a result of the integration of the three existing algorithms namely: Adaptive CUSUM algorithm, the EWMA algorithm and Naïve Bayes in order to improve the detection accuracy of DDoS attacks in Cloud Computing. The newly designed RTNTAD improved the detection rate of DDoS attacks with low false positives. Furthermore, the proposed algorithm has the capability to detect unknown attacks. The proposed RTNTAD algorithm is presented using Algorithm 1 below.

Algorithm 1: Real-Time Network Traffic Attacks Detection (RTNTAD)

1. Initialization
2. Set the detection threshold $k > 0$
3. $G_{-1} = h_{n-1} = 0$
4. $n = 0$
5. $\vartheta_n = 0$ // process mean predicted in observation real-time
6. $\tau = 0$ // factor of EWMA
7. End
8. While the algorithm is not stopped do
9. Measure the current sample $x[n]$
10. $G_i = \ln\left(\frac{d(p_i, \delta_1)}{d(p_1, \delta_0)}\right)$ // This utilized to make a choice between the hypotheses

11. $G_n = \sum_{i=0}^{n} G_i$ // The cumulative sum from 0 to n
12. $h_n = G_n - \min_{1 \le l_c \le n} G_{l_c - 1}$ // Decision function h_n
13. $\widetilde{l_c} = \frac{min}{1 \le t_c \le n} G_{l_c} - 1$ // log-probability ratio
14. $G_n = G_{n-1} + G_n$ // The equations may be rewritten in a recursive form for real-time detection of change
15. $G_n = \{G_{n-1} + S_n\}^+$ // The decision function G_n may be compared to a positive threshold
16. $h_n = \{h_{n-1} + G_n\}^+$ // decision function G_n compared to a positive threshold
17. $G_i = \frac{\emptyset_{P_1} - \emptyset_{P_0}}{\theta_P^2} \left(P_i - \frac{\emptyset_{P_1} + \emptyset_{P_0}}{2} \right)$ // Calculating log-probability proportion
18. $\bar{\vartheta}_n = \tau \bar{\vartheta}_n - 1 + (1 - \tau)$// implies that the new data supersedes the older data
19. $L(M_k|y = \frac{L(M_k) L(y|M_k)}{\sum_{i=1}^{k} L(y|M_i) L(M_i)}$ // allots the class label to given dataset based on the likelihood
20. If $h_n[n] > k > 0$ *then*
21. $l_d \leftarrow n$
22. $\widetilde{l_c} = \min_{1 \le l_c \le n} G_{l_c - 1}$
23. Stop or reset the algorithm
24. End
25. If $\tau = 1$ then
26. // Only new data may be considered
27. Else
28. If $\tau = 0$
29. // therefore, the older data are utmost imperative
30. End
31. End
32. End
33. End
34. $n = n + 1$
35. End

The proposed RTNTAD algorithm has been designed to improve the detection accuracy with minimal false positive in a way that it can DDoS attacks that enters the network they are effectively detected in real-time.

E. System Implementation

This paper designed the RTNTAD algorithm in order to detect DDoS attacks in real-time. When a malicious traffic has been detected, it is stopped immediately and an alarm signal of such attack is sent. This paper utilized MATLAB simulation tool to evaluate the performance of the proposed algorithm in Cloud Computing. The MATLAB application version R2017a was installed in a windows 10 Enterprise machine that runs 2.60GHz processor with 8192MB RAM [21].

F. Testing and Results

Simulation is another way of modelling as well as a preferred approach to understanding the real world [22]. The employment of simulation addresses the natural method of "doing while learning" [22]. Computer simulation is the disciple of planning a model of a real hypothetical framework, executing it on a computerized environment in order to analyses the execution outcome [22], [23]. Hence, a simulation was used in this study.

1. Experimental Evaluation

The CICIDS 2007 dataset was generated in MatLab in order to train ANN function and the target value. ANN is useful as it is a viable method to increase performance of IDS framework which depend on training and learning processes that can be utilized for detection of anomalies and abuse in the network [24][25]. ANN has two classes of learning process namely: supervised training approach that trains the input and output patterns as well as the unsupervised training approach that only trains the input pattern [24][25]. This study utilized the supervised training approach.

2. Simulation Results

This paper presented the simulation results based on an average of 30 simulations and focused mainly on the following parameters namely, the first parameter is the detection rate which is the effectiveness of the accuracy in detection. The second parameter is the classification of DDoS attacks which is the way to detect if the traffic contains malicious traffic and can be classified as an attack with a notification signal raised. The third parameter is the network connectivity which also affect performance of the algorithms. The final parameter is the amount of false positives (AFP) which comes if the algorithm wrongful classify the traffic as an attack.

3. The Detection Rate

The detection rate of the proposed RTNTAD algorithm was compared with that of the CUSUM, EWMA and the Naïve Bayes algorithms as described in the Fig 2. The results were analyzed when the amount of traffic was set from 4 to 40 in order to observe the performance of the detection accuracy for each algorithm. The proposed RTNTAD algorithm is not constrained by the amount of new traffic coming into the network as shown in Figure 2.

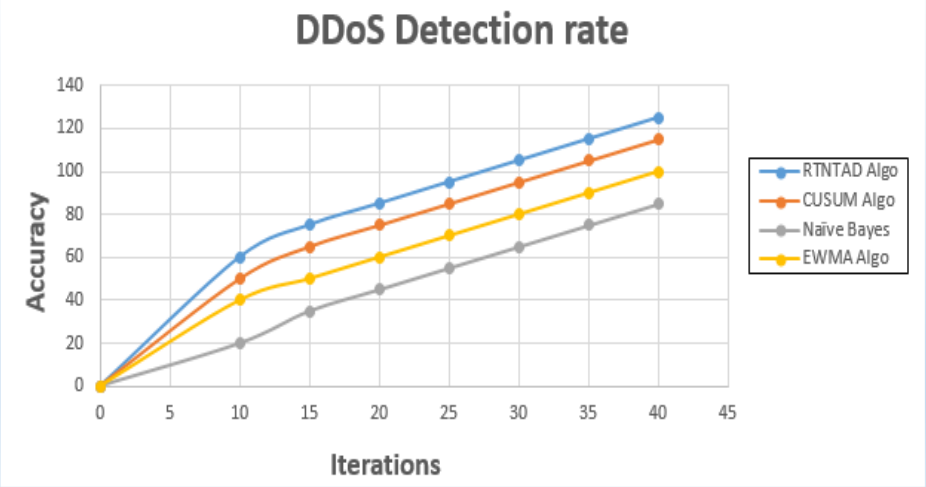

Figure 2. Detection rate comparison

The detection rate of the RTNTAD algorithm has shown good results 99.2% compared to the CUSUM algorithm that came second with 98.1%, EWMA 80% and Naïve Bayes with 79.9%. The observation is done in real-time with change in traffic load to test large amount of traffic capability and in high speed. This is for the reason that RTNTAD has the capability to detect a shift in the values of the network traffic and is easy to deploy in real-time.

4. The classification of DDoS Attacks

The classification of network traffic was conducted in order to determine if the coming traffic contains malicious traffic or not, it was observed in 40 iterations and the performance of the RTNATD came first in the detection process as shown in Figure 3.

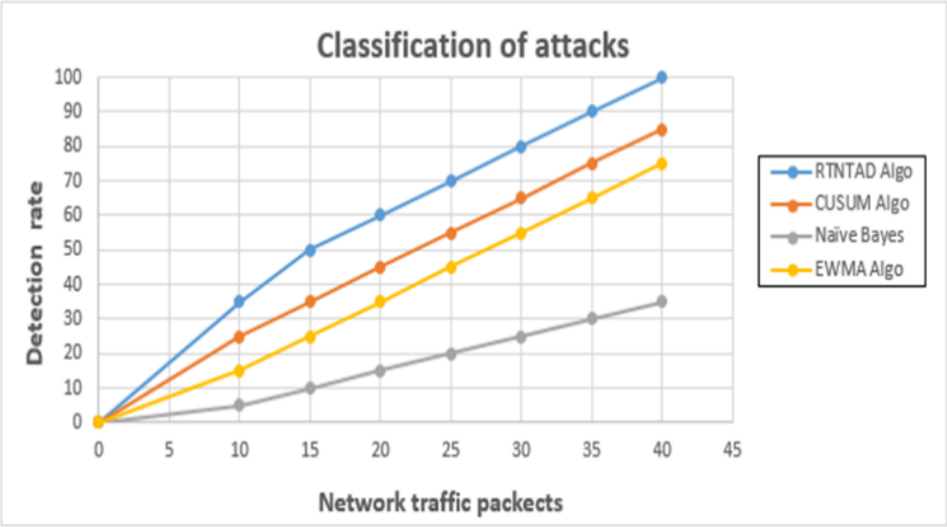

Figure 3. Traffic classification comparison

As shown in Figure 3, the RTNTAD algorithm has showing good performance over other algorithms by 99.5%. The CUSUM algorithm came second by 85.6%

below the RTNTAD algorithm, the EWMA 70% and Naïve Bayes came last with an average of 39%. This is for the reason that the RTNTAD has combined the capability of unknown detection and that of the EWMA which uses current and previous data traffic which enhance classification. Therefore, the classification of the RTNTAD becomes effective more than all other algorithms.

5. Network Connectivity

Network connectivity issues can affect performance and therefore a simulation was conducted to determine the efficiency of the performance of the algorithms through network connectivity throughput limitations as shown in Figure 4. The connectivity time out was analyzed when the throughput changes from 5 to 35 and the threshold delay was set to 15.

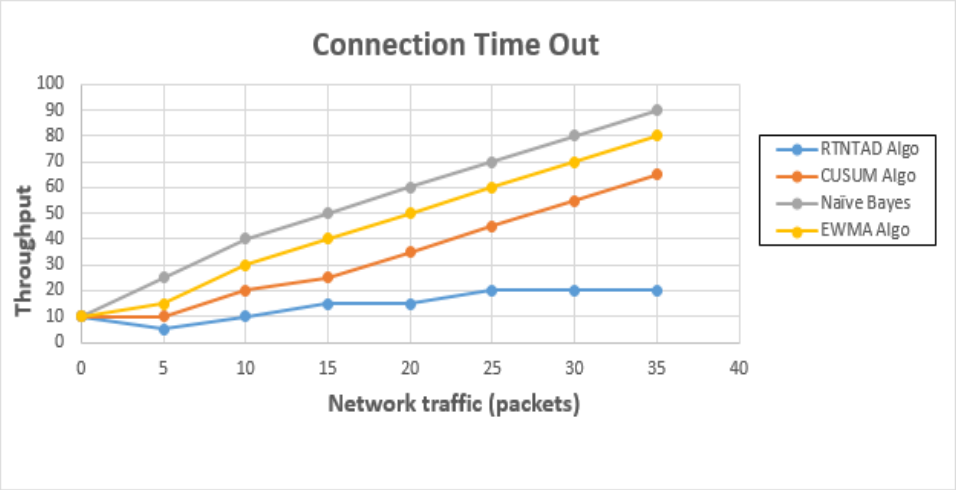

Figure 4. Connection timeout

The presented results can lead to the interpretation that the proposed RTNTAD algorithm performed well under different network limitation by 0.9%. The amount of connection time out was minimum compared to the other three algorithms of 5.9% of CUSUM, 7.9% of EWMA and 8.9% of Naïve Bayes. This include the speed of the network, the traffic volume per second and the session time out. This is for the reason that RTNTAD has improved the memory control as a result of being able to handle more than one session at a time with large amount of traffic unlike each one individually.

6. Amount of False Positive

The amount of false positive comes when the algorithm wrongfully classifies traffic as malicious attacks. The results were analyzed and presented as shown in Figure 5. Evaluations were done to determine if the proposed algorithm is capable of improving the detection of false positive.

Figure 5. Amount of false positive detection.

Based on the results shown in Figure 5, it is safe to conclude that the proposed RTNTAD algorithm improved the detection of false positives. RTNTAD algorithm achieved over 80% true positive when the simulation was repeated 30 times with less than 18% false positive while the other algorithm where still showing high number of false positive. The capability for the RTNTAD algorithm to be able to use the current and previous data traffic has increased the classification feature unlike when the algorithms are disjointed.

G. Conclusion and Future Work

This study has proposed a RTNTAD algorithm to address the pressing issue of DDoS attacks in cloud computing environments. By integrating Adaptive CUSUM, EWMA, and Naïve Bayes techniques, the RTNTAD algorithm effectively enhances detection accuracy, minimizes false positives, and operates reliably under varying traffic loads. The simulation results that the proposed algorithm can output existing solution. This demonstrate the algorithm's robustness and practicality for real-world deployment. In addition, the algorithm contributes to enhancing trust and resilience in cloud services, an essential factor as both public and private sectors increasingly migrate to cloud computing for its scalability, cost-efficiency, and flexibility.

The impact of these results is twofold: technically, the RTNTAD algorithm offers a scalable and lightweight solution for real-time DDoS detection; practically, it enhances QoS and operational resilience in cloud infrastructures that increasingly support critical public and private sector services. This positions RTNTAD as a viable security component for modern cloud systems, where service availability and reliability are paramount.

Future research will focus on further optimizing the algorithm to reduce latency and enhance performance under even more diverse network conditions. By advancing detection precision and responsiveness, this work contributes to the broader goal of building intelligent, secure, and adaptive cloud-based infrastructures capable of withstanding evolving cyber threats.

H. Acknowledgment

The authors would like to thank the Tshwane University of Technology for financial support. The authors declare that there is no conflict of interest regarding the publication of this paper.

I. References

[1] Shaar, F. & Efe, A., 2022. DDoS Attacks and Impacts on Various Cloud Computing Components. International Journal of Information Security Science, Vol. 7, No. 1, pp. 26-48.

[2] Alomari, E., Gupta, B. B. & Karuppayah, S., 2012. Botinet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art. International Journal of Computer Applications Vol. 49, No. 7, pp. 24-32.

[3] Amjad, A., Alyas, T., Farooq, U. & Tariq, M. A., 2019. Detection and Mitigation of DDoS attack in Cloud Computing using machine learning algorithm. EAI Endorsed Transactions on Scalable Information Systems, Vol. 6, No. 23, pp 1-8.

[4] Dong, S., Abbas, K. & Jain, R., 2019. A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing. IEEE Access, Vol. 7, No. 10, pp. 80813-80828.

[5] Sen, J., 2013. Security and Privacy Issues in Cloud Computing, Innovation Labs, pp. 1-42.

[6] Bharot, N., Verma, P., Suraparaju, V. & Gupta, S., 2016. Mitigating Distributed Denial of Service Attack in Cloud Computing Environment using Threshold based Technique. Indian Journal of Science and Technology, Vol. 9, No. 38, pp. 1-7.

[7] Krishna, U. L. & Kumar, M. M. V. M., 2018. Detecting Distributed Denial-of-Service Flooding Attacks using Detection and Defense Algorithm. International Journal of Creative Research Thoughts, Vol. 6, No. 1, pp. 1495-1503.

[8] Mahjabin, T., Xiao, Y., Sun, G. & Jiang, W., 2017. A Survey of distributed denial-of-service attack, prevention, and mitigation techniques. International Journal of Distributed Sensor Networks, Vol. 13. No, 12, pp. 1-33.

[9] Alzahrani, S. & Hong, L., 2018. A Survey of Cloud Computing Detection Techniques against DDoS Attacks. Journal of Information Security, Vol.9, No. 1, pp. 45-69.

[10] Virupakshar, K.B., Asundi, M., Channal, K., Shettar, P., Patil, S. & Narayan, D.G., 2020. Distributed Denial of Service (DDoS) Attacks Detection System for OpenStack-based Private Cloud. International Conference on Computational Intelligence and Data Science (ICCIDS 2019). pp. 2297-2307

[11] Somasundaram, A. & Meenakshi, V. S., 2021. DDoS Mitihation In Cloud Computing Environment By Dynamic Resource Scaling With Elastic Balancing. Turkish Journal of Computer and Mathematics Education, Vol.12, No.11, pp. 3346-3362.

[12] Awan, M.J., Farooq, U., Babar, H.M.A., Yasin, A., Nobanee, H., Hussain, M., Hakeem, O. & Zain, A.M., 2021. Real-Time DDoS Attack Detection System Using Big Data Approach. Sustainability 2021, Vol. 13, No. 19, pp. 1-19.

[13] Zekri, M., Kafhali, S. E., Aboutabit, N. & Saadi, Y., 2017. DDoS Attack Detection Using Machine Learning Techniques in Cloud Computing Environment.

International Conference of Cloud Computing Technologies and Applications (CloudTech), pp. 1-7.
[14] Wang, B., Zheng, B., Lou, W. & Hou, T. Y., 2014. DDoS Attack Protection in the Era of Cloud Computing and Software-Defined Networking. IEEE 22nd International Conference on Network Protocols, Vol. 81, No, 1, pp. 624-629.
[15] Abbas, S.A. Almhanna, M.S., 2021. Distributed Denial of Service Attacks Detation System by Machine Learning Based on Dimensionality Reduction. Journal of Physics: Conference Series.
[16] Bhaya, W. & EbadyManaa, M., 2017. DDoS attack detection approach using an efficient cluster analysis in large data scale. Proceedings of 2017 Annual Conference on New Trends in Information &Communications Technology Applications (NTICT), pp. 168-173
[17] Zhang, H., Dai, S., Li, Y. & Zhang, W., 2018. Real-time Distributed-Random-Forest-Based Network Intrusion Detection System Using Apache Spark. IEEE 37th International Performance Computing and Communications Conference (IPCCC), pp.1-7.
[18] Yin, C., Zhu, Y., Fei, J. & He, X., 2017. A Deep Learning Approach for Detection Using Recurrent Neural Networks, IEEE Acess vol. 5, No. 1, pp. 21954-21961.
[19] Abdulrahman, A.A. & Ibrahem, M. K., 2018. Evaluation of DDoS Attacks Detection in a CICIDS2017 Dataset Based on Classification Algorithms. Iraqi Journal of Information and Communications Technology ((IJICT), Vol. 1, No. 3, pp. 49-55.
[20] Ying, B., 2014. CUSUM-Based Intrusion Detection Mechanism for Wireless Sensor Networks, Journal of Electrical and Computer Engineering, Vol. 2, No. 1, pp. 1-6.
[21] Valdiviezo, L.M., 2014. Simulation Models for the Evaluation of Detection and Defense Protocols against Cyber Attacks Preparation of Doctoral Consortium Contributions, International Conference on Simulation and Modeling, Vol. 17, No. 1, pp. 42-47.
[22] Stancic, H., Seljan, S., Centinic, A. & Sankovic, D., 2007. Simulation Models in Education, Digital Information and Heritage, pp. 469-481.
[23] Fishwick, P.A., 1995. Computer Simulation: The Art and Science of Digital World Construction. pp. 1-9.
[24] Norwahidayah, S., Farahah, N.N., Amirah, A., Liyana, N. & Suhana, N., 2021. Performances of Artificial Neural Network (ANN) and Particle Swarm Optimization (PSO) Using KDD Cup '99 Dataset in Intrusion Detection System (IDS), Journal of Physics: Conference Series, pp. 1-8.
[25] Baloyi, D. P. Du Plessis, T. E. Mathonsi and Tshilongamulenzhe T. M., 2022. Implementation of an Enhanced Security Algorithm for Detecting Distributed Denial of Services Attacks in Cloud Computing, 2022 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 2022, pp. 953-957, doi: 10.1109/CSCI58124.2022.00170.