International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6320
***Article Received**: 28 December 2022 **Revised**: 30 January 2023 **Accepted**: 10 February 2023*

Enriched Model of Case Based Reasoning and Neutrosophic Intelligent System for DDoS Attack Defence in Software Defined Network based Cloud

A. Lavanya[1], N.Shanmuga Priya[2]
[1]Research Scholar
Dr.SNS Rajalakshmi College of Arts and Science
Coimbatore, Tamil Nadu 641049,India
Emil: lavanyasamymsc@gmail.com
[2]Head, Department of Computer Applications (PG)
Dr.SNS Rajalakshmi College of Arts and Science
Coimbatore, Tamil Nadu 641049,India
Email:spriyanatrajan@gmail.com

Abstract-- Software Defined Networking in Cloud paradigm is most suitable for dynamic functionality and reduces the computation complexity. The routers and switches located at the network's boundaries are managed by software-defined netwrking (SDN) using open protocols and specialised open programmable interfaces. But the security threats often degrade the performance of SDN due to its constraints of resource usage. The most sensitive components which are vulnerable to DDoS attacks are controller and control plane bandwidth. The existing conventional classification algorithms lacks in detection of new or unknown traffic packets which are malicious and results in degradation of SDN performance in cloud resources. Hence, in this paper double filtering methodology is devised to detect both known and unknown pattern of malicious packets which affects the bandwidth of the control panel and the controller. The case-based reasoning is adapted for determining the known incoming traffic patterns before entering the SDN system. It classifies the packets are normal or abnormal based on the previous information gathered. The traffic patterns which is not matched from the previous patterns is treated as indeterministic packet and it is defined more precisely using the triplet representation of Neutrosophic intelligent system. The grade of belongingness, non-belongingness and indeterminacyis used as the main factors to detect the new pattern of attacking packets more effectively. From the experimental outcomes it is proved that DDoS attack detection in SDN based cloud environment is improved by adopting CBR-NIS compared to the existing classification model.

Keywords: DDoS attacks, Indeterminacy, neutrosophic intelligent system, Case based reasoning, Software defined network.

I.INTRODUCTION

In order to share knowledge and resources through digital information technology,networking has become an integral element of our life. It involves digitally conversing with other gadgets. However, the static architecture of the conventional networkconnections makes it impossible to reconfigure the new policies and regulations because they are not adaptable [1]. This is because data and control planes are tightly coupled, which implies that the hardware and software used for data forwarding have embedded controlling and routing policies[2]. The dynamic management of the network and its protocols is made more challenging.The commercial sector of today benefits greatly from cloud computing. The use of software, technologies, and resources in the cloud enables the provision of a variety of services [3]. The majority of businesses started to incorporate cloud services by paying for service usage.

In addition, service providers must satisfy the needs of commercial clients. Network virtualization is necessary to constructprogrammable networks and adaptable to meet the time-sensitive requirements of emerging applications [4]. Software-defined networking (SDN) is a novel pattern that was developed to provide the future generation model required to overcome the limitations of current networks[5].

This renders forwarding devices less intelligent. They function like standard forwarding devices.The distinct feature of SDN distinguishes it from conventional networking solutions, which tightly integrate the control and data planes. With this strategy, all operation is managed by coding without requiring any adjustments to the network infrastructure architectures. SDN only performs rule or policy improvements in the control plane if they are required as a result of user requests, which reduces computation cost[6].

II.SECURITY CHALLENGES IN SDN

When the usage of SDN based cloud networking paradigm has expanded, the security threats against SDN to impair its normal operations. The network topology provided by the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6320
***Article Received**: 28 December 2022 **Revised**: 30 January 2023 **Accepted**: 10 February 2023*

controller is centrally viewed by SDN. It is, however, exposed to a multitude of hazards because of this trait. By modifying the controller, an attacker has various opportunities to alter how the entire SDN network functions.Due to some architectural flaws, SDN is exposed to a number of security risks [7].The impact of the security flaws in the SDN design are

- Due to limitations in flow table memory, the open flow switches are unable to accumulate all the rules to flow when new inward packets arrived and results to DDoS attacks.
- In SDN, security risks are caused by the controller's single port of breakdown and downstream failure.
- Control plane and data plane communicate by open flow, so there is a high chance of DDoS attacks by disturbing the communication to choke bandwidth of switch-controller.
- Switches in SDN depends on the regulator to take the proper behaviour while forwarding data. Because of the high volume of traffic, this feature of Routers and switches may cause the efficiency of the controller and regulate plane bandwidth to decrease.

Instead of detecting the DDoS attack detecting after it enters inside the system, it is very important to predict whether the incoming packets are malicious or benign. Hence, machine learning becomes most promising technology in prediction and mitigation of DDoS Attacks. Hence in this proposed work double filtering method is devised to handle both known and unknown attacks to enhance the functionality of SDN based cloud environment performance.

III.RELATED WORK

This section discusses about the few of the existing modes that use machine learning and mining approaches for DDoS attack detection in SDN.

Muhammad Imran et al [8] conducted a detailed study on various mitigation and classification of malicious traffic in SDN environment due to DDOS attacks. In their investigation mitigation strategies and limitation are discussed.

Chen et al [9] devised an exciting gradient boosting model to detect DDOS attack in SDN topology detection archetypal using flow packet dataset. The POX is used as SDN controller with the aid of Mininet. The scalability and accuracy of known attack detection is improved.

Sufian Hameedet al [10] developed a secure controller to controller algorithm which permits to communicate the controller very securely by forwarding attack information to others. This provides effective traffic filtering close to the attack source and efficient warning along the route of an active attack, conserving significant time and shared network.

Zheng et al [11] introduced a Reinforcing Anti-DDoS Actions in real-time usednovel correlation investigation to perceive and stifle DDoS attacks and is based on unmodified commercially available SDN switches. A variety of flooding-based DDoS attacks can be effectively defended against by using this approach.

Khashab et al [12] suggested a strategy employing machine learning to automatically detect and prevent assaults in SDN networks. It uses the original flow properties alone to identify attacks. The studies' findings showed that the most successful ML algorithm is RF. This work does not factor in the unidentified patterns.

Myint Oo et al [13] in their work improvised the conventional support vector machine to recover the malicious action. They detected two kinds of DDOS attack based on flooding. The advanced Support vector machine works as a multiclass classification algorithm which uses volumetric and asymmetric characteristics as signifies features during DDoS attack detection.

Itagiet al [14] developed a centralised controller to detect DDoS attack in SDN. The incoming data traffic are classified using bidirectional recurrent neural network. The class imbalance in detection of unknown attacks are challenging.

Gumaste et al [15] focused on developing a lightweight algorithm to handle the denial of service attack with the concept of dynamic time series. They introduced SDN manager to forecast the prediction of bandwidth accuracy.

Tao et al[16] devised a real time DDoS attack discovery model with help of machine learning classifiers. OpenStack based cloud testbed is used for evaluation the detection technique. The random forest classifier is used to classify whether the income packets are normal or malicious.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6320
***Article Received**: 28 December 2022 **Revised**: 30 January 2023 **Accepted**: 10 February 2023*

IV.METHODOLOGY: ENRICHED MODEL OF CASE BASED REASONING AND NEUTROSOPHIC INTELLIGENT SYSTEM FOR DDOS ATTACK DEFENCE IN SDN BASED CLOUD

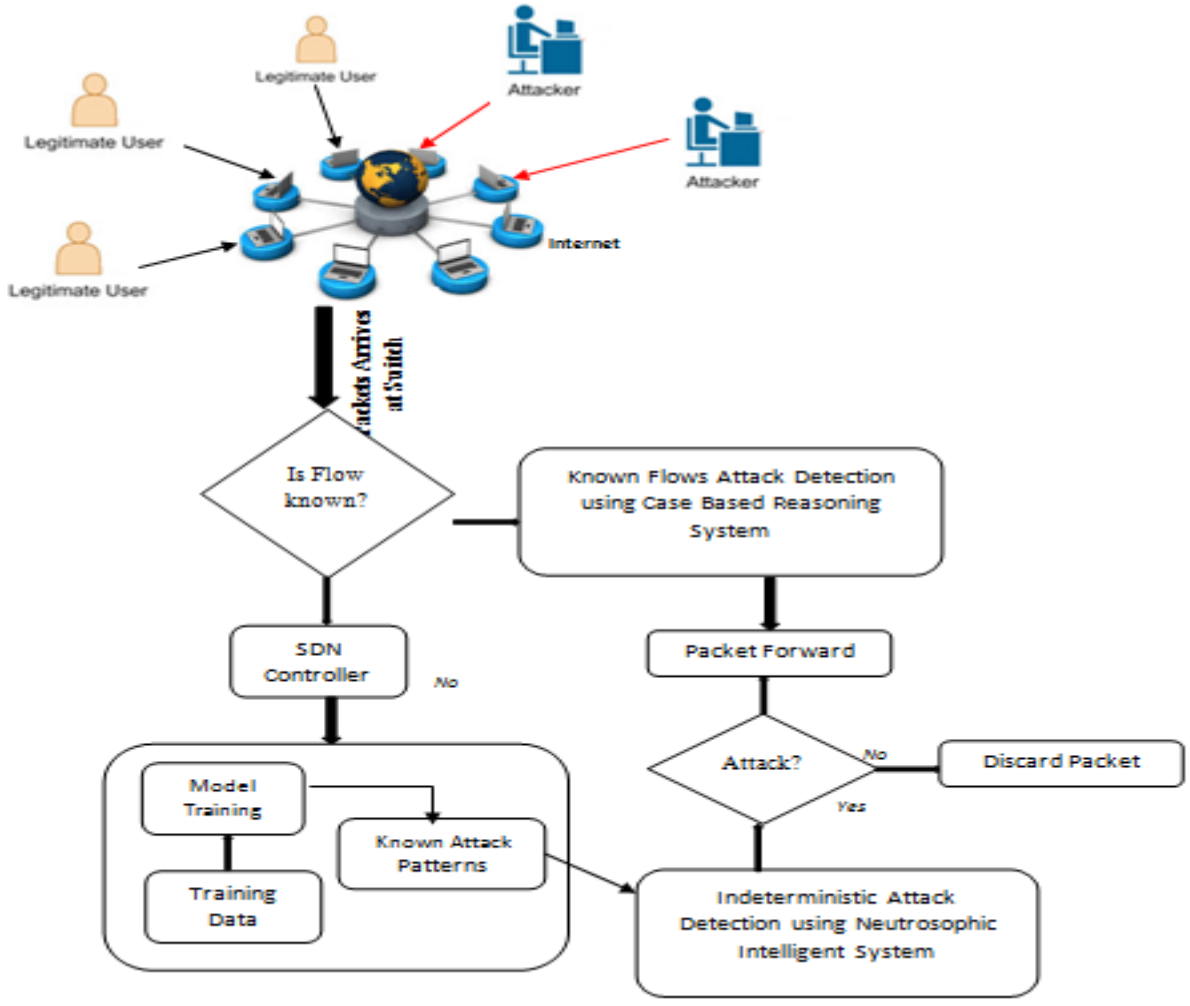

Figure 1: Overall Architecture of the Case based Reasoning integrated Neutrosophic Inference System

In this proposed model handing the class imbalance to identify the DDoS attacks that affect the SDN controller. It uses the historical database information and discover the matching traffic patterns and eradicate them to stop entering inside the SDN. The known pattern of DDOS attack is detected by applying the case-based reasoning method which uses the previous attacking patterns and alleviates them from entering inside the system. The new and unknown pattern of traffic patterns are well handled by the Neutrosophic Intelligent System, which defines the input data based on belongingness towards truthfulness, falsity, indeterminacy. The indeterminate values of packets are considered as new or unknown packets and they are eliminated from the network. The two-level filtering of incoming packets in SDN based controller optimize the process of detecting known and unknown attacks very effectively. The complete work flow is depicted in the figure 1.

Case Based Reasoning System

In present days, security provinces experience more knowledge on types of attacks, detection, prevention and prediction of possibility of vulnerability threats on Software Designed Network which consequences to complexity in attack detection. An intelligence-based learning method called Case Based Reasoning was developed by Roger Shank in accordance with cognitive theories, much like how humans react based on analogical reasoning. In order to verify similar cases from the case base, CBR compares the query case to prior cases. The remaining comparable examples are used to help solve brand-new cases. Additionally, the newly discovered case is kept as a case base's incremental learning model for forecasting.

The most effective method which utilizes the previous acquired knowledge for understanding the incoming patterns is termed as Case Based Reasoning (CBR). It is self-adaptive

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6320
***Article Received**: 28 December 2022 **Revised**: 30 January 2023 **Accepted**: 10 February 2023*

and capable of learning how to address new problems. For multifaceted decision making CBR enacts very cautiously for security mechanism when the situation is uncertainty facts. There may be issues with the assessment method or with optimization. With the aid of CBR, inter networks can combine their learning content and make decisions. Figure 2 depicts the process of CBR cycle.

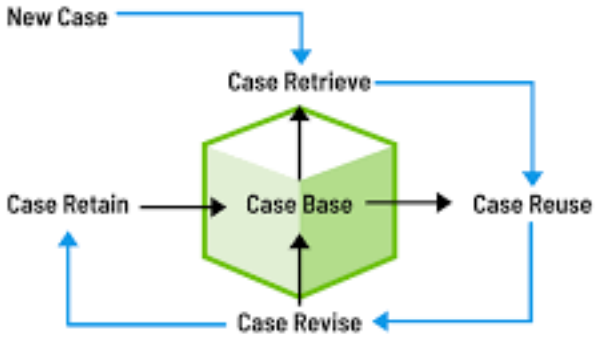

Figure 2:Process of CBR cycle

The CBR helps to solve most of the unfamiliar traffic patterns by analysing previously classified patterns. Form the knowledge acquire by the historical traffic patterns with the class labels as normal or abnormal, the action will be taken on specific incoming packets. The results from the previously handled concerns are codified as instances, and each instance provides a feature descriptive of the issue and its associated response. The particular instance keeps a record of the instances in the database and serves as a knowledge foundation for dealing with known issues.The model is continually being improved in order to forecast events more correctly as experience and understanding grow. In general, the CBR approach consists of four components: a case base to store historical data, a search indexing mechanism, a matching algorithm to assess similarity, and lastly an adaptation mechanism.

The following diagram illustrates the steps involved in CBR: extract, utilize, update, and preserve:

- Extract: To determine the type of a particular query instance, retrieve relevant cases from cache.
- Utilize: Map the relevant prior case for a specific query record to address the issue.
- Update: While previous records has been planned to the query instance, test the newly provided in the actual world and make any necessary revisions.
- Preserve: Accumulate the learned knowledge as a new-fangledevent in reminiscence once the query instance has adjusted the results.

Neutrosophic Intelligent System for unknown attack Discovery

Figure 4 exposes the uncertainty inference engine which encompassed of Neutrosophical components that receives incomingdata packets and allocates appropriate belongingness grade towards truthfulness, indeterministic and falseness. The Inference engine of neutrosophical values that plots both input and output values and Deneutrosophicationcomponents plansNeutrosophication converted to real values.

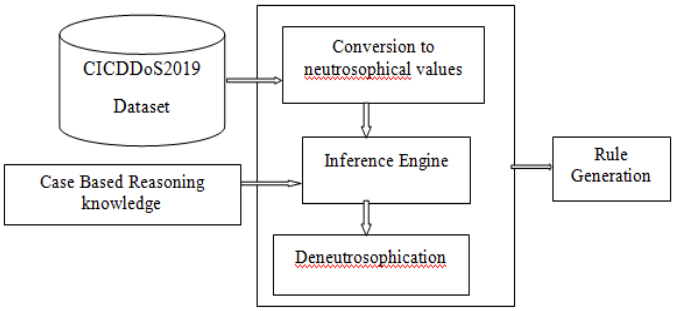

Figure 3: Unknown attack pattern detection using Neutrosophic Model

In Neutrosophication, the elements represented in terms of truthiness, falsity and indeterminateness are not dependent to each other. The figure 4 depicts neutrosophic membership representation. Each of these factors are denoted in a single valued triangular membership function is used and the representation is denoted as $R_{\mathbb{N}}$ = (Δ1, Δ2, Δ3; Ω1, Ω2, Ω3; Ψ1, Ψ2, Ψ3) the degree of truthiness, falsity and indeterministic value are formulated as shown below:

$$\mu_{R_{\mathbb{N}}}(w) = \begin{cases} \frac{w-\Delta_1}{\Delta_2-\Delta_1}; & \Delta_1 \le w < \Delta_2 \\ 1 \ ; & w = \Delta_2 \\ \frac{\Delta_3-w}{\Delta_3-\Delta_2}; & \Delta_3 < w \le \Delta_2 \\ 0 \ ; & else \end{cases}$$

$$\pi_{R_{\mathbb{N}}}(w) = \begin{cases} \frac{\Omega_2-w}{\Omega_2-\Omega_1}; & \Omega_1 \le w < \Omega_2 \\ 0 \ ; & w = \Omega_2 \\ \frac{w-\Omega}{\Omega_3-\Omega_2}; & \Omega_2 < w \le \Omega_3 \\ 1 \ ; & else \end{cases}$$

$$\vartheta_{R_{\mathbb{N}}}(w) = \begin{cases} \frac{\Psi_2-w}{\Psi_2-\Psi_1}; & \Psi_1 \le w < \Psi_2 \\ 0 \ ; & w = \Psi_2 \\ \frac{w-\Psi 1}{\Psi_3-\Psi 2_2}; & \Psi_2 < w \le \Psi_3 \\ 1 \ ; & else \end{cases}$$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6320
***Article Received**: 28 December 2022 **Revised**: 30 January 2023 **Accepted**: 10 February 2023*

where, $0 \leq \mu_{R_{\mathbb{N}}}(w) + \pi_{R_{\mathbb{N}}}(w) + \vartheta_{R_{\mathbb{N}}}(w) \leq 3$, $w \in R_{\mathbb{N}}$.

The neutrosophic representation of an instances is

$$(R_{\mathbb{N}})h, l, k = [\mu_{\mathbb{N}1}(h), \mu_{\mathbb{N}2}(h);\ \pi_{\mathbb{N}1}(l), \pi_{\mathbb{N}2}(l);\ \vartheta_{\mathbb{N}1}(k), \vartheta_{\mathbb{N}2}(k)]$$

where,

$\mu_{\mathbb{N}1}(h) = \Delta_1 + h\,(\Delta_2 - \Delta_1)$

$\mu_{\mathbb{N}2}(h) = \Delta_3 - h\,(\Delta_3 - \Delta_2)$

$\pi_{\mathbb{N}1}(l) = \Omega_2 - l\,(\Omega_2 - \Omega_1)$

$\pi_{\mathbb{N}2}(l) = \Omega_2 + l\,(\Omega_3 - \Omega_2)$

$\vartheta_{\mathbb{N}1}(k) = \Psi_2 - k\,(\Psi_2 - \Psi_1)$

$\vartheta_{\mathbb{N}2}(k) = g_2 + k(\Psi_3 - \Psi_2)$

here, $0 < h \leq 1$, $0 < l \leq 1$, $0 < k \leq 1$ and $0 < h + l + k \leq 3$

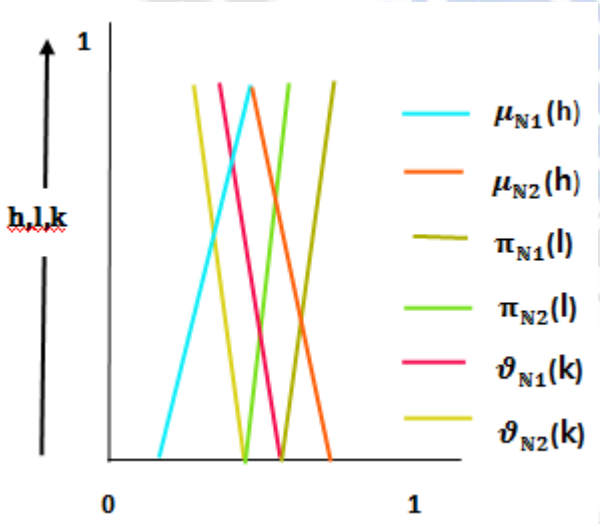

Figure 4:Neutrosophical values of belonginess, non-belongingness and indeterministic

Rule Generation of NIS

Every instance of network traffic data packet has embodied as normal, malicious and indeterminacy. Each traffic packets contain n + 1 features which defines the type of packets. The first n featuresdefine the characteristics of the traffic packet and the additional feature defines the labels of each record. The set of rules generated by Neutrosophy inference engine has a group of neutrosophic rules to discriminate the input details of a packet as normal, abnormal and indeterminacy class.

RL1: IF $cond_1$ THEN data is $cls\text{-}pkt_1$ . . .

RLn: IF $condi_m$ THEN data is $cls\text{-}pkt_n$

Few of the neutrosophic rules for DDoS attack detection in SDN are:

IF pktcoun is low and tot_dur is low pktrate is low and pktperflow is average and tot_kbps is average then packet is normal

IF pktcoun is average and tot_dur isaverage pktrate is high and pktperflow is average and tot_kbps is low then packet is indeterministic

IF pktcoun is high and tot_dur ishigh pktrate is high and pktperflow is high and tot_kbps is average then packet is malicious.

V.EXPERIMENTAL RESULTS

This section discusses in detail about the perforamnce analysis of the proposed case based reasosning and Case Based Reasoning and Neutrosophic Intelligent System for DDoS defence technique in SDN based cloud environment. The dataset is collected from CICDDoS2019 [20]it comprised of traffic patterns details of both benign and DDOS attacks. The python software is used for simulating CBR-NIS to predict the DDoS attack and it is compared with Association rule mining and support vector machine to detect the known pattern of DDos attacks. To discover the unknown pattern of attacks fuzzy inference system and rule induction classifier is used. The evaluation metrics used are Detection Rate (DR), Accuracy, False Alarm Rate, abnormal packet detection, packet drop ratio and End to End delay.

Testing Conduction

The experiment was conducted in a runtime environment using MINNitsimulator whichgenerates virtual hosts associated to OVS switch. The network is controlled by POX, aPython-based SDN controller. The Python-based Scikit-learn machine learning libraries were used for the evaluation on a Windows 10 operating system with Intel(R) Core(TM) i5-6200U CPU, 2.30GHz and 8.00 GB RAM. The Number of packets used are 5000, Number of Nodes: 100 and the Type of Cloud: Hybrid Cloud.

The figure 5 shows the number of attack request in SDN based cloud environment, which shows the normal and abnormal number of requests.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6320
***Article Received**: 28 December 2022 **Revised**: 30 January 2023 **Accepted**: 10 February 2023*

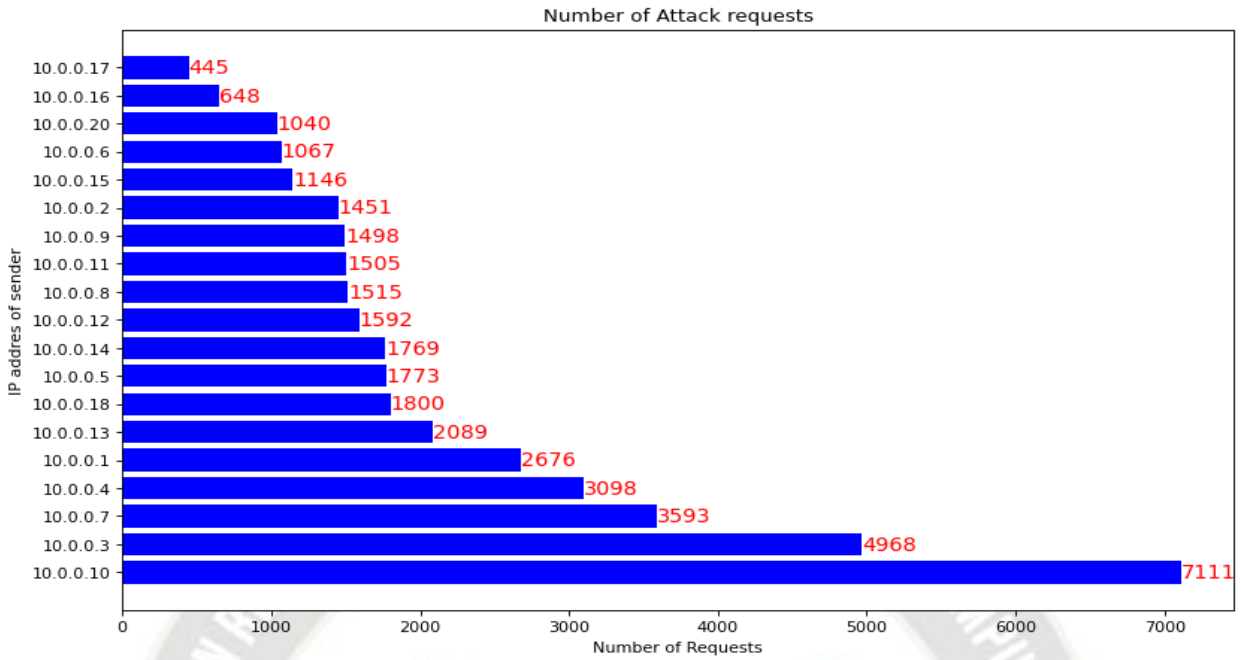

Figure 5 Number of attack request vs IP address of sender

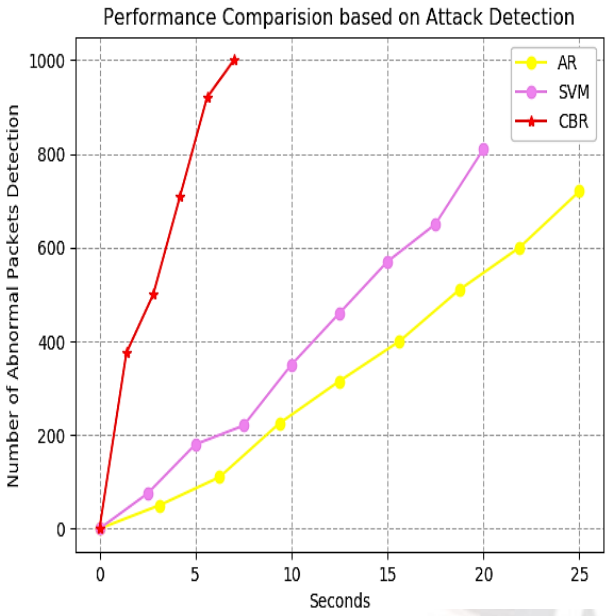

Figure: 6 Comparison based on Abnormal packets detection

Figure 6 explores abnormal packets detection rate by three different algorithms to prevent DDOS attack defence in Software Designed Network driven cloud environment. The proposed algorithm case-based reasoningachieves highest detection of abnormal packets compared to existing association rule and support vector machine algorithms. Case Based Reasoning (CBR) model, uses its retrieve, reuse, revise and retain policies to match the incoming packets with the historical packets for determining similar pattern and classifying the incoming packets as normal or malicious in case of known patterns. The support vector and association rule classifiers due to high class imbalance it results in overfitting problem, result in low detection rate compared to CBR for Distributed denial of service attack discovery in SDN.

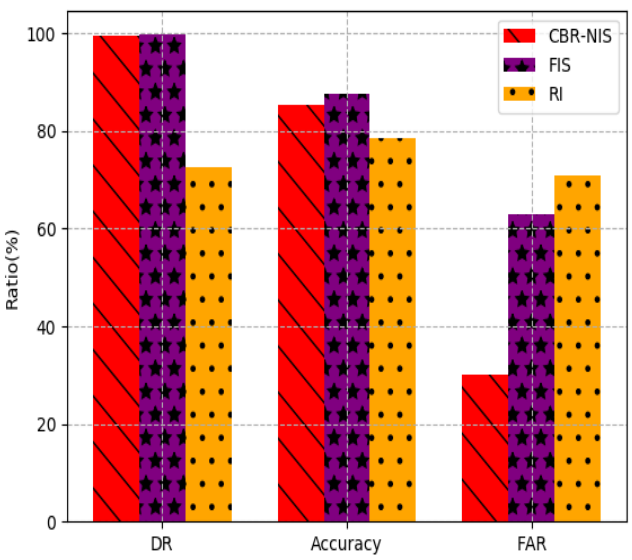

Figure 7: Performance analysis based on DR, Accuracy and FAR

The figure 7 explores the efficiency of the case-based reasoning for pattern understanding and neutrosophic inference model for uncertainty handling (CBR-NIS) based on detect rate, accuracy and false alarm rate. The proposed CBR-NIS tackles the issue of class imbalance among normal traffic pattern and abnormal traffic patterns with the usage of

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6320
***Article Received**: 28 December 2022 **Revised**: 30 January 2023 **Accepted**: 10 February 2023*

historical information. The unknown attacking packets are provided further attention and it is precisely defined by uncertainty logic known as neutrosophic inference system. The NIS represents each characterizes of a packet in three different grades of belongingness towards truthiness, falsity and indeterminacy based on normal and abnormal packets. While using fuzzy inference system it defines each packets in terms of membership grade only, the rule induction classifier suffers from class imbalance and they produce less result compared to the proposed CBR-NIS algorithm for DDoS attack detection in SDN based cloud.

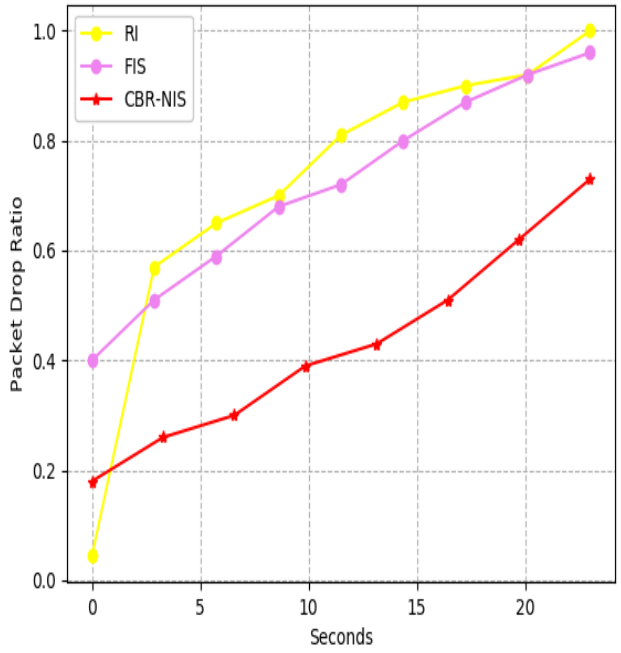

Figure 8: Performance Comparison based on Packet Drop Ratio

The packet drop ratio explores the ability of the defence mechanisms of three different algorithms used in this research to detect DDoS attack in SDN as shown in figure 8. The known pattern of malicious packets is detected by the examining the historical data about the abnormal traffic patterns using case based reasoning method. The new or unknown attacks are the major challenge in SDN to reduce the packet drop ratio. Hence, in this work Neutrosophication is applied to define each characteristic of incoming traffic as triplet representation towards degree of belongingness. So that, indeterminacy in classifying incoming packet with unknown traffic patterns as malicious or normal is intelligently handled. Hence, the proposed CBR-NIS considerably reduced the packet drop ratio compared to conventional FIS and RI.

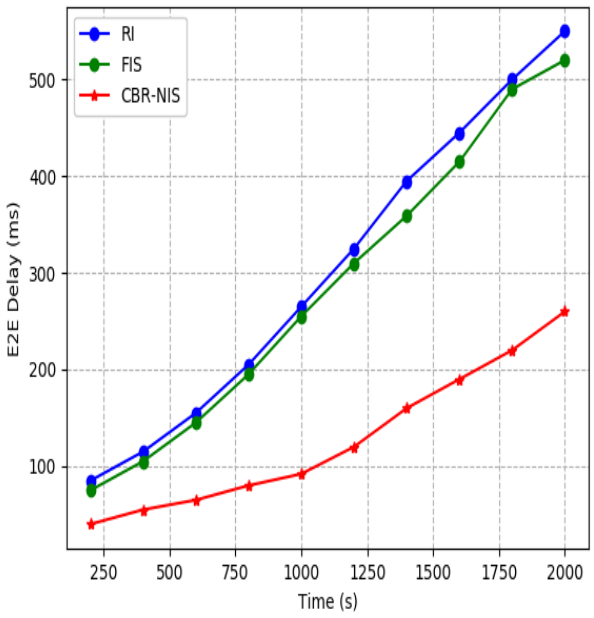

Figure 9: Comparative analysis of End to End Delay

The end-to-end delay based comparative assessment of proposed CBR-NIS, FIS and RI for DDoS attack detection in SDN is depicted in the figure 9. When the SDN in cloud environment is in the process of data transfer, the attack on any of the cloud node which involves in transmission path results in packet loss. If the cloud environment is protected with strong security mechanism the packet drop ration can be effectively controlled. Hence, the proposed CBR-NIS acts as a security filtering mechanism which discards the malicious incoming packets before entering inside the SDN system whether it is known or unknown attacks. Thus, the end to end delay due to abnormal traffic generated by DDOS attacks is interpreted in terms of tristate degrees using Neutrosophication theory and produced best result compared to the conventional algorithms.

VI. Conclusion

The proposed algorithm focused on handling indeterministic pattern of DDoS attack detection in SDN based cloud environment. The proposed case-based reasoning integrated neutrosophic inference system is introduced in this work to handle both unknown and indeterministic traffic patterns which affects the performance of the SDN based system. The controller decision is improvised in this work using neutrosophical representation of each parameters in dataset in terms of belongingness, non-belongingness and indeterminacy values. The simulation results proved the prominence of proposed CBR-NIS compared with other existing state of arts Rule Induction and fuzzy Inference system. The involvement of historical data-based filtering of known pattern of attacks mainly reduces the computation

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6320
***Article Received**: 28 December 2022 **Revised**: 30 January 2023 **Accepted**: 10 February 2023*

complexity of the CBR-NIS and improves the DDoS attack detection rate in SDN based cloud.

REFERENCES

[1] B. Rashidi, C. Fung, and E. Bertino, ``A collaborative DDoS defence framework using network function virtualization," IEEE Trans. Inf. Forensics Security, vol. 12, no. 10, pp. 2483_2497, 2017.

[2] Q. Yan, W. Huang, X. Luo, Q. Gong, and F. R. Yu, ``A multi-level DDoS mitigation framework for the industrial Internet of Things," IEEE Commun. Mag., vol. 56, no. 2, pp. 30_36, 2018.

[3] Sindia, Dhas, Julia. (2017). SDN based DDoS attack detection and mitigation in cloud. International Journal of Control Theory and Applications. 10. 39-47.

[4] Yuhua Xu, Yunfeng Yu, Hanshu Hong, Zhixin Sun, "DDoS Detection Using a Cloud-Edge Collaboration Method Based on Entropy-Measuring SOM and KD-Tree in SDN", Security and Communication Networks, vol. 2021, pages 12, 2021.

[5] G. Kaur and P. Gupta, "Classifier for DDoS attack detection in software defined networks," Internet of Things in Business Transformation: Developing an Engineering and Business Strategy for Industry 5.0, vol. 20, pp. 71–90, 2021

[6] Yu, S., Zhang, J., Liu, J. et al. A cooperative DDoS attack detection scheme based on entropy and ensemble learning in SDN. J Wireless Com Network 2021, 90 (2021).

[7] P. T. Dinh and M. Park, "BDF-SDN: A Big Data Framework for DDoS Attack Detection in Large-Scale SDN-Based Cloud," *2021 IEEE Conference on Dependable and Secure Computing (DSC)*, 2021, pp. 1-8.

[8] Muhammad Imran, Muhammad Hanif Durad, Farrukh Aslam Khan, Abdelouahid Derhab, Towardan optimal solution against denial of service attacks in software defined networks. Future GenerationComputer Systems, 92 pages :444–453, 2019

[9] Z. Chen, F. Jiang, Y. Cheng, X. Gu, W. Liu and J. Peng, "XGBoost Classifier for DDoS Attack Detection and Analysis in SDN-Based Cloud," 2018 IEEE International Conference on Big Data and Smart Computing (BigComp), 2018, pp. 251-256,

[10] Sufian Hameed, Hassan Ahmed Khan, SDN based collaborative scheme for mitigation of DDoS attacks.Future Internet, 10(3), 2018.

[11] J. Zheng, Q. Li, G. Gu, J. Cao, D. K. Y. Yau,J. Wu, Realtime DDoS defense using cots SDN switches via adaptive correlation analysis, IEEE Transactions on Information Forensics and Security,13(7):1838–1853, 2018.

[12] F. Khashab, J. Moubarak, A. Feghali and C. Bassil, "DDoS Attack Detection and Mitigation in SDN using Machine Learning," 2021 IEEE 7th International Conference on Network Softwarization (NetSoft), 2021, pp. 395-401

[13] M. Myint Oo, S. Kamolphiwong, T. Kamolphiwong S. Vasupongayya, "Advanced Support Vector Machine-(ASVM-) Based Detection for Distributed Denial of Service (DDoS) Attack on Software Defined Networking (SDN)", Journal of Computer Networks and Communications, vol. 2019, pp. 1-12, 2019

[14] V. Itagi, M. Javali, H. Madhukeshwar, P. Shettar, P. Somashekar and D. G. Narayan, "DDoS Attack Detection in SDN Environment using Bi-directional Recurrent Neural Network," *2021 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER)*, 2021, pp. 123-128.

[15] S. Gumaste, D. G. Narayan, S. Shinde and K Amit, "Detection of DDoS attacks in OpenStack-based private cloud using apache spark", *J. Telecommun. Inf. Technol*, vol. 4, pp. 62-71, Jan. 2021

[16] Tao Wang, Hongchang Chen, Guozhen Cheng, Yulin Lu, "SDNManager: A Safeguard Architecture for SDN DoS Attacks Based on Bandwidth Prediction", Security and Communication Networks, vol. 2018, Article ID 7545079, 16 pages, 2018

[17] Chantamit-o-pas, Pattanapong & Goyal, Madhu. (2018). A Case-Based Reasoning Framework for Prediction of Stroke. 10.1007/978-981-10-5508-9_21.

[18] F. Smarandache, "Definition of Neutrosophic Logic – A Generalization of the Intuitionistic Fuzzy Logic", Proceedings of the Third Conference of the European Society for FuzzyLogic and Technology, EUSFLAT 2003, September 10-12, 2003, Zittau, Germany; University of Applied Sciences at ZittauGoerlitz, 141- 146.

[19] Smarandache, Florentin. "A Unifying Field in Logics: Neutrosophic Logic". Philosophy (1999): 1-141.

[20] https://www.unb.ca/cic/datasets/ddos-2019.html