Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 5 (2023)

Analysis Of DDOS Attack Detection In Cloud Computing Using Machine Learning Algorithm

[1] Sathish Polu, [2]Dr.V.Bapuji

[1]Research scholar, Bir Tikendrajit University
[2]Research Supervisor, Bir Tikendrajit University

Abstract: The proliferation of cloud computing has revolutionized the landscape of digital services, offering scalability and flexibility. However, this evolution has also exposed cloud environments to a heightened risk of Distributed Denial of Service (DDoS) attacks, threatening the availability and reliability of hosted services. This research presents a comprehensive analysis of DDoS attack detection in cloud computing, leveraging the capabilities of machine learning algorithms. The study involves the collection and preprocessing of network traffic data within a cloud environment. Relevant features are selected to characterize normal and anomalous activities. Machine learning algorithms, including but not limited to Support Vector Machines (SVM), Random Forests, and Decision Trees, are explored for their efficacy in distinguishing DDoS attacks from legitimate traffic. Furthermore, the research investigates the impact of varying dataset sizes and feature sets on the performance of the detection models.

Background:

Distributed Denial of Service (DDoS) attacks in the context of cloud computing represent a significant cybersecurity challenge due to the unique characteristics of cloud environments. Understanding the background of these attacks is crucial for devising effective mitigation strategies. Cloud computing has transformed the way businesses and individuals access and manage computing resources. It offers scalability, flexibility, and cost-effectiveness, making it a popular choice for hosting applications and services. Cloud computing relies on the pooling of computing resources, enabling multiple users (tenants) to share the same infrastructure. This multi-tenancy introduces complexities and challenges in securing the environment. As organizations increasingly migrate their operations to the cloud, the reliance on cloud services for critical business functions has grown. Any disruption to these services can have severe consequences. Some DDoS attacks are politically or socially motivated, aiming to disrupt services to convey a message or protest. Business rivals might launch DDoS attacks to gain a competitive edge by disrupting the services of a competitor. Attackers may demand payment to stop a DDoS attack, threatening to disrupt services if their demands aren't met. The shared nature of cloud resources means that an attack on one tenant can impact others, leading to collateral damage. The ability of cloud services to dynamically scale resources based on demand also provides attackers with the means to amplify the scale of DDoS attacks. DDoS attacks have evolved in sophistication, with attackers employing tactics like amplification and reflection to maximize the impact of their assaults. Techniques such as DNS amplification, SYN/ACK floods, and HTTP-based attacks are commonly used to overwhelm cloud services. DDoS attacks aim to disrupt the availability of services, leading to downtime and potential financial losses for businesses. The reputational damage from prolonged service disruptions can be substantial, affecting customer trust and confidence. Cloud service providers and organizations deploy various mitigation strategies, including traffic filtering, rate limiting, and the use of Content Delivery Networks (CDNs) to absorb and distribute malicious traffic. Understanding the background of DDoS attacks in cloud computing is essential for developing proactive security measures, incident response plans, and collaborations between cloud service providers and their customers to enhance the overall resilience of cloud environments against these evolving threats. Establishing a baseline of normal network behaviour and flagging deviations as potential DDoS attacks. Examining patterns in network flows, such as sudden spikes or unusual distribution, to identify anomalies. Utilizing predefined signatures or patterns associated with known DDoS attacks. This method identifies attacks by matching the observed traffic patterns against a database of known attack signatures. Analysing deviations from expected network protocols to identify and block malicious traffic. Applying statistical models to network traffic metrics (e.g., packet rates, bandwidth usage) to identify deviations from the established baseline, signalling potential DDoS attacks. Using machine learning

techniques to detect abnormal patterns in network behaviour, which may indicate a DDoS attack. Algorithms can adapt to evolving attack strategies. Monitoring the rate of incoming traffic and imposing rate limits. Sudden spikes in traffic trigger the detection mechanism. Identifying and blocking malicious packets based on characteristics commonly associated with DDoS attacks. Employing heuristics to identify unusual behaviours in network traffic. This may involve looking for patterns that deviate from the expected norm. Analysing user interactions and behaviours to detect anomalies that may indicate a DDoS attack, particularly in web applications. Introducing challenges, such as CAPTCHAs or token-based validations, to differentiate between legitimate users and automated attackers. This technique helps filter out malicious traffic. Distributing content across multiple servers globally to absorb and filter malicious traffic closer to the source. Diverting traffic through specialized services that filter out malicious requests before reaching the target. Understanding these theoretical aspects is essential for developing comprehensive DDoS detection strategies that can effectively identify and mitigate attacks in real-world scenarios. The combination of these techniques is often employed to create robust defence mechanisms against the evolving landscape of DDoS threats.

Challenges and Opportunities:

Streaming data, also known as real-time data, presents both challenges and opportunities when combined with machine learning (ML) techniques. Here's an overview of the key challenges and opportunities associated with streaming data and ML:

Challenges:

1. Volume and Velocity:

- Challenge: Streaming data often comes in large volumes at high velocities, making it challenging to process and analyse in real-time.
- Opportunity: ML algorithms need to be designed to handle the high influx of data, and the real-time nature of streaming data can lead to more timely and actionable insights.

2. Latency:

- Challenge: Low latency is critical in streaming data applications, and traditional batch processing ML models may not be suitable for real-time requirements.
- Opportunity: ML models optimized for streaming data, such as online learning algorithms, can provide real-time predictions and insights.

3. Concept Drift:

- Challenge: Data distribution in streaming applications can change over time (concept drift), making it necessary to continuously adapt ML models.
- Opportunity: Adaptive and online learning algorithms can help ML models adjust to changes in the data distribution, ensuring ongoing model accuracy.

4. Data Quality and Anomalies:

- Challenge: Streaming data may contain noise, outliers, or missing values, which can impact the performance of ML models.
- Opportunity: ML models can be augmented with anomaly detection techniques to identify and handle irregularities in the data.

5. Scalability:

- Challenge: As the volume of streaming data increases, ensuring the scalability of ML models and infrastructure becomes crucial.
- Opportunity: Distributed computing frameworks and cloud-based solutions can be leveraged to scale ML models horizontally and handle large volumes of streaming data.

Opportunities:

1. Real-time Decision Making:

- Opportunity: Streaming ML enables organizations to make decisions in real-time, allowing for quicker responses to changing conditions and opportunities.

2. Personalization and Adaptation:

- Opportunity: Streaming data allows for continuous learning and adaptation of ML models, leading to more personalized and context-aware predictions or recommendations.

3. Early Detection of Patterns:

- Opportunity: ML models applied to streaming data can identify emerging patterns or trends early, enabling proactive decision-making and intervention.

4. Reduced Storage Requirements:

- Opportunity: Streaming data applications can reduce the need for storing large volumes of historical data, focusing on the most recent and relevant information for ML model training.

5. Dynamic Model Updating:

- Opportunity: Streaming ML enables dynamic model updates in response to changes in the data distribution, ensuring that models remain relevant and accurate over time.

6. Integration with IoT and Sensors:

- Opportunity: Streaming ML is well-suited for applications in the Internet of Things (IoT) and sensor networks, where real-time insights are crucial for monitoring and control.

In summary, while streaming data with ML presents challenges related to data volume, velocity, and dynamic nature, it also opens up opportunities for real-time decision-making, continuous learning, and early pattern detection. Successful implementation requires careful consideration of the specific characteristics of the streaming data and the design of ML models tailored for real-time processing.

Methodology:

Cloud computing has upset the manner in which associations store, process, and deal with their information, offering savvy and versatile answers for a great many applications. In any case, the rising dependence on cloud administrations has made them alluring focuses for cybercriminals. Among different digital dangers, Conveyed Refusal of Administration assaults have arisen as a huge test, making serious interruption cloud-based benefits, and influencing the accessibility and dependability of assets. DDoS assaults are ordinarily sent off by overpowering designated frameworks with enormous measures of traffic from different sources, making it challenging for the framework to recognize authentic and pernicious solicitations. The effect of DDoS assaults can be crushing, prompting significant monetary misfortunes, reputational harm, and loss of client trust. Thusly, early location and moderation of DDoS assaults are vital for guaranteeing the security and accessibility of cloud administrations. In various regions, for example, perceiving pictures, regular language handling, and digital protection, profound learning calculations have had astonishing outcomes. These calculations can possibly learn complex examples and connections inside information, making them appropriate for identifying DDoS assaults in cloud conditions.

- **Random Forest:**

Random Forest is an ensemble learning algorithm that can be applied to various machine learning tasks, including DDoS attack detection. In the context of DDoS detection, Random Forest can be utilized to analyse network traffic patterns and classify them as normal or malicious. Random Forest is an ensemble learning algorithm that builds multiple decision trees during training and merges them to get a more accurate and stable prediction. Each tree is constructed by selecting a random subset of features at each node and making decisions based on those features. The final prediction is determined by a majority vote among all trees. Random Forest randomly selects a subset of features for each decision tree. In the context of DDoS detection, these features could include network traffic metrics, packet rates, protocol types, etc. Random subsets of the training data are sampled with replacement to create different datasets for each tree. Decision trees are constructed using the selected features and training data. During the classification phase, each decision tree "votes" on the class (normal or DDoS) based on the features of a given input (e.g., network traffic data). The final prediction is determined by a majority vote among all the decision trees in the Random Forest. Random Forest tends to be less prone to overfitting compared to individual decision trees. Effective in scenarios with a large number of features, making it suitable for analysing diverse network traffic metrics. Define relevant features for DDoS detection, such as packet rates, traffic volume, and protocol distribution. Use labelled datasets containing instances of normal and

DDoS traffic for training. Once trained, the Random Forest model can be applied to analyse real-time network traffic and classify it as normal or potentially part of a DDoS attack. Assess the performance of the Random Forest model using metrics such as accuracy, precision, recall, and F1 score. Employ techniques like cross-validation to ensure robustness and generalizability. Random Forest's ability to handle diverse features and mitigate overfitting makes it a valuable tool for DDoS detection, particularly in the complex and dynamic environment of network traffic analysis. It is important to fine-tune the model parameters and validate its performance on relevant datasets for optimal results.

- **Support Vector Machine (SVM)**

Support Vector Machine (SVM) is a supervised machine learning algorithm that can be applied to various classification tasks, including DDoS attack detection. SVM is particularly effective in situations where the decision boundary between classes is not linear and exhibits complex patterns. SVM is primarily a binary classification algorithm, meaning it is used to separate data into two classes. SVM finds the optimal hyperplane (decision boundary) that maximally separates the instances of different classes in the feature space. These are the data points that lie closest to the decision boundary and play a crucial role in determining the optimal hyperplane. SVM can handle non-linear decision boundaries by transforming the input features into a higher-dimensional space using kernel functions. Define relevant features for DDoS detection, such as packet rates, traffic patterns, or other network metrics. Use labelled datasets containing instances of normal and DDoS traffic for training. SVM identifies the hyperplane that maximizes the margin between different classes. Effective for non-linear decision boundaries and commonly used in DDoS detection to capture complex patterns. Define relevant features that capture the characteristics of normal and DDoS traffic. Depending on the nature of the data, choose an appropriate kernel function. Once trained, the SVM model can be applied to analyse real-time network traffic and classify it as normal or potentially part of a DDoS attack. Assess the performance of the SVM model using metrics such as accuracy, precision, recall, and F1 score. Use techniques like cross-validation to ensure robustness and generalizability. SVM performs well in scenarios with a high number of features. SVM is less prone to overfitting, particularly with appropriate kernel selection. SVM's ability to handle non-linear decision boundaries and its effectiveness in high-dimensional spaces make it a valuable tool for DDoS attack detection. Proper parameter tuning, kernel selection, and validation on relevant datasets are essential for optimizing its performance in the context of DDoS detection.

- **Deep Sequential Model**

A deep sequential model refers to a type of neural network architecture that is designed to process sequential or time-series data. These models are particularly effective in tasks where the order and timing of input data are crucial for making accurate predictions or classifications. In the context of DDoS attack detection in cloud computing or network security, a deep sequential model can be beneficial for capturing temporal patterns and dependencies in network traffic data. DDoS attacks often involve patterns that unfold over time, making sequential data processing crucial for detection. RNNs, a type of deep sequential model, are designed to maintain a memory of previous inputs, enabling them to capture temporal dependencies in sequential data. Traditional RNNs may suffer from the vanishing gradient problem, limiting their ability to capture long-term dependencies. LSTMs are a specialized type of RNN that addresses the vanishing gradient problem by introducing memory cells, allowing the network to retain information over longer sequences. LSTMs use gating mechanisms to control the flow of information into and out of the memory cells. GRUs are another type of gated recurrent network that simplifies the architecture compared to LSTMs while maintaining effectiveness in capturing sequential patterns. Input features could include various network traffic metrics, such as packet rates, protocol distribution, and other time-series data. The model is trained on labelled datasets to learn the temporal patterns associated with normal and DDoS traffic. Once trained, the deep sequential model can be applied to analyse real-time network traffic, identifying patterns indicative of DDoS attacks. Assessment metrics should consider the temporal nature of the data, including metrics like precision, recall, and F1 score. Techniques like time-based cross-validation ensure that the model generalizes well to unseen temporal patterns. Deep sequential models can capture long-term dependencies and contextual information in sequential data, enhancing the ability to detect subtle DDoS patterns. These models can adapt to changing attack strategies and evolving network behaviour. Deep sequential models,

particularly LSTMs and GRUs, have demonstrated success in various time-series prediction tasks and are well-suited for applications where understanding temporal patterns is critical, such as DDoS attack detection in network security. The effectiveness of these models depends on the quality and relevance of the input features and the availability of labelled data for training.

- **Long Short-Term Memory Networks**

Long Short-Term Memory (LSTM) networks are a type of recurrent neural network (RNN) architecture designed to overcome the limitations of traditional RNNs in capturing long-range dependencies in sequential data. LSTMs are particularly effective in processing and predicting sequences of data, making them well-suited for applications like time-series analysis, natural language processing, and, as relevant to your question, DDoS attack detection in network security. LSTMs incorporate memory cells, which allow them to maintain information over longer sequences. This addresses the vanishing gradient problem that plagues traditional RNNs, enabling LSTMs to capture dependencies over extended time horizons. Determines which information from the previous state should be discarded. Decides which new information to incorporate into the memory cell. Determines the output based on the current input and the memory cell's content. LSTMs process sequential data one element at a time, updating their internal state and memory cells based on the input at each time step. LSTMs are trained using backpropagation through time, a variant of the backpropagation algorithm adapted for sequential data. This involves updating the model's weights by considering the entire sequence during training. LSTMs can be fed with various network traffic metrics, such as packet rates, protocol distribution, and other time-series data, to capture temporal patterns associated with normal and DDoS traffic. LSTMs are trained on labelled datasets, learning to recognize temporal patterns indicative of DDoS attacks. The ability to capture long-term dependencies is crucial for detecting subtle attack patterns. Once trained, LSTMs can be applied to analyse real-time network traffic, continuously updating their internal state to identify deviations from normal behaviour that may signal a DDoS attack. Performance metrics such as precision, recall, F1 score, and area under the ROC curve can be used to assess the model's effectiveness in detecting DDoS attacks. LSTMs excel at capturing long-term dependencies in sequential data, making them suitable for detecting subtle and evolving DDoS attack patterns. LSTMs can adapt to changing attack strategies and evolving network behaviour, enhancing their robustness in dynamic environments. LSTMs are well-suited for tasks involving time-series data, aligning with the temporal nature of network traffic in DDoS attack scenarios. LSTM networks, with their ability to capture temporal dependencies and process sequential data effectively, have shown promise in enhancing the capabilities of DDoS attack detection systems, contributing to improved accuracy and adaptability in identifying malicious network behaviour.

- **Radial basis function (RBF) Neural Network**

The Radial Basis Function (RBF) Neural Network is a type of artificial neural network that employs radial basis functions as activation functions. RBF networks are particularly well-suited for pattern recognition, function approximation, and classification tasks. Radial basis functions are used as activation functions in the hidden layer of the network. The most common choice is the Gaussian function. The output of a radial basis function is determined based on the distance between the input vector and a centre associated with that function.

Three Layers:

-Input Layer: Represents the input features (e.g., network traffic metrics) that are fed into the network.

- Hidden Layer: Contains radial basis functions with learnable parameters (centroids and widths) that process the input data.

- Output Layer: Performs the final classification or regression based on the transformed features from the hidden layer. Centroids and widths of the radial basis functions are learned during the training phase. The centroids represent the centres of the radial basis functions, and the widths control the spread of these functions. The training of an RBF Neural Network typically involves a two-step process: Centroids can be initialized randomly or using a clustering algorithm. Weights and widths are adjusted using methods like gradient descent to minimize the difference between the predicted and actual outputs. Input features can include various network traffic metrics relevant to DDoS attack detection, such as packet rates, protocol distribution, and other time-series data. RBF Neural Networks can learn complex temporal patterns associated with both normal and DDoS network

behaviour. Once trained, the RBF Neural Network can be applied to real-time network traffic for the detection of patterns indicative of DDoS attacks. Standard classification metrics such as accuracy, precision, recall, and F1 score can be used to evaluate the performance of the network in distinguishing between normal and attack traffic. RBF Neural Networks are inherently non-linear, enabling them to capture complex patterns in the data, which is beneficial for detecting intricate DDoS attack patterns. RBF Neural Networks can effectively handle high-dimensional feature spaces, making them suitable for tasks involving diverse network traffic metrics. These networks can adapt to evolving attack strategies and changing network conditions, enhancing their robustness. RBF Neural Networks offer a unique approach to DDoS attack detection, leveraging radial basis functions to transform and process input data effectively. However, successful application and performance depend on appropriate feature selection, proper network architecture design, and careful parameter tuning during the training phase.

- **Hybrid LSTM WITH RBF Model**

Making a hybrid model that joins a LSTM (Long Transient Memory) organization and a Spiral Premise Capability Brain Organization (RBFNN) is an intriguing thought. The fundamental thought is to utilize the LSTM to handle consecutive information and catch worldly conditions, while the RBFNN can deal with the non-direct connections and insert between data of interest.

Data Preprocessing:

Dataset:

The CICDDoS datasets have been gathered by network safety involving Wireshark in demonstrated situations. They comprise of two unique examples of purpose, different DoS, and DDoS assaults, notwithstanding various stage's assaults. The data gathered is pre-handled utilizing the CIC Stream Meter. It highlights 88 web traffic capacities that produce different DDoS and DoS assaults traffic insights. The information gathered from the assortment, and saved in CSV design, incorporates a variety of traffic components. We utilize an organization of bots to send a gigantic measure of settled inquiries to an IP once an individual plays out a DNS-based DDoS obliteration. In a LDAP-based assault, an assailant makes solicitations to a compromised server which is accessible to everybody to produce huge reactions that are in this way communicated to the frameworks being gone after. This dataset contains an assortment of current reflected DDoS assaults, including PortMap, NetBIOS, LDAP, MSSQL, UDP, UDP-Slack, SYN, NTP, DNS, and SNMP assaults.

Data Preprocessing:

It is one of the main methodology before information investigation. Notwithstanding significant measures of indispensable and helpful data, crude information likewise contains a sizable amount of clamour, copy values, missing qualities, mistake, and so on. In this way, it is vital to work on the nature of the crude information to support the viability and straightforwardness of information examination. Information pre-handling makes this essentially and effectively conceivable. The information pre-handling process utilizes a few systems for different objectives. Information purging has been utilized in this undertaking as a pre-handling step for the information. Information cleaning, otherwise called information scouring or information cleaning, is a handling technique used to distinguish botches in crude information, eliminate copies, fill in spaces, or eliminate mistaken information. The CICDDoS2019 dataset is in CSV design and incorporates an immense number of information parcels. To guarantee that the example is arbitrary, the strategy for irregular testing is utilized while bringing in the information. Since these sections don't have a mathematical worth and instead contain boundless, these columns of information are taken out from the dataset. The arrangement of information had been diminished by 17 elements with little effect on precision. To arrange DDoS assaults, the informational collection has been isolated into two gatherings: harmless and assaults. " Harmless" is doled out the worth "0" in the dataset made for perceiving an organization assault, while different assaults are set to "1." For order purposes, the assault techniques have been separated into two essential gatherings: assaults in view of abuse and goes after in light of reflection. For reasons for grouping, reflection-based assaults, and abuse based dangers were separated into

unmistakable classes. The information is standardized to carry it into the 0-1 territory and sent through the LSTM to get rebuilding.

Fig 6. Comparison of output metrics of different models

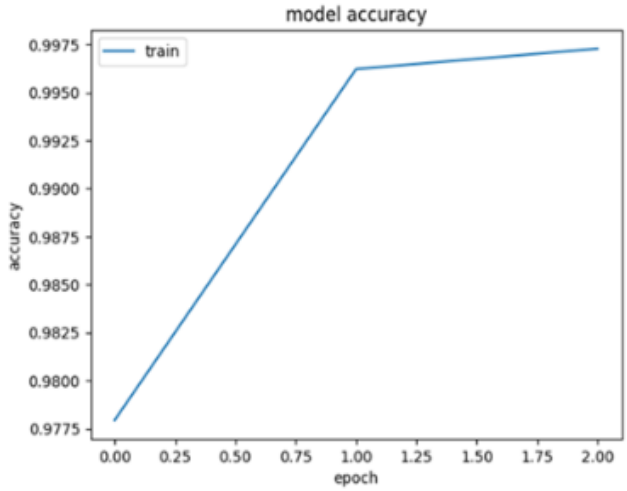

Fig 7. Epochs and loss within a plot

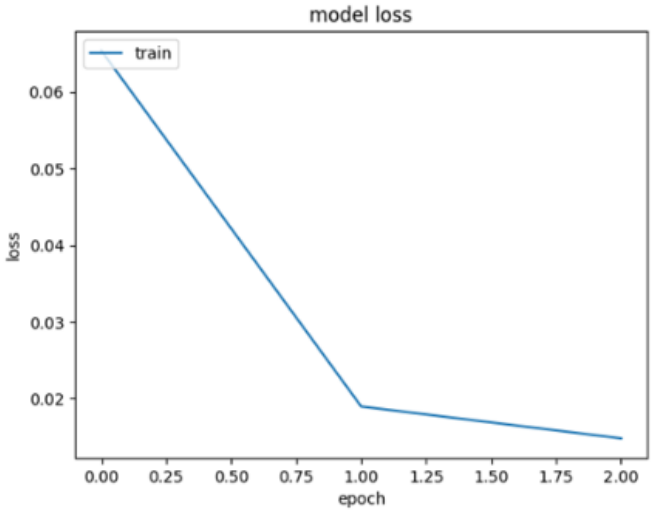

Fig 8. Plot combining Epochs and Accuracy

Conclusion:

Results provide insights into the strengths and limitations of the employed machine learning algorithms in the context of DDoS attack detection. The findings contribute to the refinement of existing detection strategies and offer guidance for the selection of optimal algorithms based on specific cloud computing scenarios. The outcomes of this research aim to enhance the resilience of cloud computing infrastructures against DDoS threats, providing a foundation for future developments in the field of cybersecurity. The analytical framework presented herein serves as a valuable resource for practitioners, researchers, and organizations seeking to fortify their cloud-based services against the evolving landscape of cyber threats.

References:

[1] Rawashdeh, A., Alkasassbeh, M., and Al-Hawawreh, M.: 'An anomaly-based approach for DDoS attack detection in cloud environment', International Journal of Computer Applications in Technology, 2018, 57, (4), pp. 312-324

[2] Wani, A.R., Rana, Q., Saxena, U., and Pandey, N.: 'Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques', in Editor (Ed.)^(Eds.): 'Book Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques' (IEEE, 2019, edn.), pp. 870-875

[3] Idhammad, M., Afdel, K., and Belouch, M.: 'Detection system of HTTP DDoS attacks in a cloud environment based on information theoretic entropy and random forest', Security and Communication Networks, 2018, 2018

[4] Hezavehi, S.M., and Rahmani, R.: 'An anomaly-based framework for mitigating effects of DDoS attacks using a third party auditor in cloud computing environments', Cluster Computing, 2020, pp. 1-19

[5] R. K. Gupta et al., "An Improved Secure Key Generation Using Enhanced Identity-Based Encryption for Cloud Computing in Large Scale 5G", Wireless Communications and Mobile Computing 2022.

[6] Khuphiran, Panida, et al. "Performance comparison of machine learning models for DDOS attacks detection." 2018 22nd International Computer Science and Engineering Conference (ICSEC). IEEE, 2018.

[7] Farnaaz, Nabila, and M. A. Jabbar. "Random forest modelling for network intrusion detection system." Procedia Computer Science 89 (2016): 213-217.

[8] Sahi, A., Lai, D., Li, Y., and Diykh, M.: 'An efficient DDoS TCP flood attack detection and prevention system in a cloud environment', IEEE Access, 2017, 5, pp. 6036-6048

[9] Chen, Z., Jiang, F., Cheng, Y., Gu, X., Liu, W., and Peng, J.: 'XG Boost classifier for DDoS attack detection and analysis in SDN-based cloud', in Editor (Ed.)^(Eds.): 'Book XGBoost classifier for DDoS attack detection and analysis in SDN-based cloud' (IEEE, 2018, edn.), pp. 251-256

[10] Kingma, D. P., & Ba, J. (2015). Adam: a method for stochastic optimization. 3rd International Conference for Learning Representations, San Diego. Sharafaldin, I., Lashkari, A. H., Hakak, S., & Ghorbani, A. A. (2019).

[11] Cheng, J.; Yin, J.; Liu, Y.; Cai, Z.;Wu, C. DDoS attack detection using IP address feature interaction. In Proceedings of the IEEE International Conference on Intelligent Networking and Collaborative

Systems, Thessalonika, Greece, 24–26 November 2010; IEEE: Piscataway Township, NJ, USA, 2009; pp. 113–118.

[12] Wang, C.; Zheng, J.; Li, X. Research on DDoS attacks detection based on RDF-SVM. In Proceedings of the 10th International Conference on Intelligent Computation Technology and Automation, Changsha, China, 9–12 October 2017.

[13] Prathyusha, D.J., and Kannayaram, G.: 'A cognitive mechanism for mitigating DDoS attacks using the artificial immune system in a cloud environment', Evolutionary Intelligence, 2020, pp. 1-12

[14] Rabbani, M., Wang, Y.L., Khoshkangini, R., Jelodar, H., Zhao, R., and Hu, P.: 'A hybrid machine learning approach for malicious behaviour detection and recognition in cloud computing', Journal of Network and Computer Applications, 2020, 151, pp. 102507

[15] Zareapoor, M., Shamsolmoali, P., and Alam, M.A.: 'Advance DDOS detection and mitigation technique for securing cloud', International Journal of Computational Science and Engineering, 2018, 16, (3), pp. 303-310