International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

MITIGATING DDOS ATTACK IN IOT NETWORK ENVIRONMENT

Dr.Kishore Kumar Gajula[1], Gangisetty Falki[2], Goudi Rithika[3], Gourishetty Sreeja[4]
[1]Associate Professor, School of CSE,Malla Reddy Engineering College For Women (UGC-Autonomous), Maisammaguda,Dhulapally,Secunderabad,Telangana-500100
[234]UG Student, School of CSE,Malla Reddy Engineering College for Women, (UGC-Autonomous), Maisammaguda,Dhulapally,Secunderabad,Telangana-500100

ABSTRACT
This paper introduces a new approach for detecting Distributed Denial of Service (DDoS) attacks using an entropy-based method. DDoS attacks are a major threat to network security, as they overwhelm target systems with a massive volume of malicious traffic, disrupting normal operations and causing service outages. Traditional detection methods, such as signature-based techniques or anomaly detection, often struggle to identify new or unknown attack types, especially zero-day attacks. In contrast, our method uses entropy measures to assess the randomness and unpredictability of network traffic, enabling us to spot abnormal patterns that suggest a DDoS attack.By calculating entropy for different network traffic characteristics—like packet size, inter-arrival time, and protocol distribution—our approach can effectively detect deviations from normal traffic, which may signal a DDoS attack. To improve detection accuracy and efficiency, we also incorporate machine learning techniques that learn from historical data to distinguish between normal and attack traffic.
Through extensive testing on real-world network datasets, we show that our entropy-based method is not only effective at detecting DDoS attacks but also minimizes false positives. This approach offers a promising solution for enhancing network security by enabling early detection and timely response to DDoS threats, helping to protect critical network infrastructure and services.
Keywords: Distributed Denial of Service (DDoS),Network security,Entropy-based detection,Traffic analysis,Anomaly detection,Attack detection ,Inter-arrival time,Protocol distribution,Early detection,Cybersecurity

I.INTRODUCTION

As the number of Internet users and the demand for online services continue to rise, the reliance on the Internet for critical services also increases. This has led to a significant rise in the damage caused by network attacks. Among these, Denial of Service (DoS) attacks have become a major concern in recent years, resulting in substantial losses for victims in terms of service quality. In a DoS attack, the attacker seeks to prevent legitimate users from accessing online resources, such as websites, web services, or computer systems. In the case of a Distributed Denial of Service (DDoS) attack, the attacker uses compromised computers, often referred to as "zombies," to generate an overwhelming amount of requests aimed at disrupting or degrading the normal service of the targeted system. A notable example of such an attack occurred in February 2014, when a massive DDoS attack hit EU-US-based servers. Security companies reported this as one of the most powerful attacks of its kind.One of the main challenges in addressing DDoS attacks is the lack of effective traceback methods to identify and track attackers quickly and efficiently after the attack. The automated nature of many DDoS attacks makes them particularly dangerous. Once an attacker identifies vulnerable systems, it can take less than five seconds to deploy an attack tool, and it only takes a minute for thousands of compromised hosts to join the attack. Tools such as Trin00, TFN, Tribe Flood Network 2000 (TFN2K), and Stacheldraht are

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

often used to launch increasingly stealthy DDoS attacks.Most current methods for detecting DDoS attacks rely on static threshold approaches, which tend to have lower detection accuracy. Additionally, some detection methods are computationally expensive, making them complex and slower to implement. To address these issues, the proposed detection method improves accuracy by using an adaptive threshold algorithm. To reduce computational complexity, we employ a fast entropy approach based on flow data, which is more efficient than traditional entropy methods.

II.RELATED WORK

DDoS attack detection generally focuses on three primary approaches: Signature-Based Approach (SBA), Anomaly-Based Approach (ABA), and Entropy-Based Approach (EBA).

In the Signature-Based Approach, system attributes are compared against a database of known malicious threats or signatures, similar to how antivirus software detects malware. The main challenge with SBA is the delay between the discovery of a new threat and the update of the signature database. During this gap, new threats can remain undetected. While SBA is efficient and easy to implement, it has limitations such as the updating lag and an inability to detect zero-day attacks. Research has shown that signature-based intrusion detection systems can identify known attacks with a low rate of false negatives, but they are not effective against unknown or newly emerging threats.

To address these limitations, the Anomaly-Based Approach was introduced. This method uses statistical analysis, data mining, and distribution analysis to monitor network traffic and compare it to an established baseline of what is considered "normal" for the network. The baseline includes typical bandwidth usage, commonly used protocols, and regular port and device connections. When traffic deviates significantly from this baseline, the system alerts the administrator to potential anomalies. However, one of the challenges with ABA is the risk of generating false positives. If the baseline is not carefully configured, legitimate changes in network usage may trigger an alarm.

Entropy-Based Approaches, on the other hand, offer significant advantages in detecting DDoS attacks. In normal network conditions, the entropy values for various features remain relatively stable. However, during an attack, the entropy values of one or more network features can change drastically. The use of entropy enhances the sensitivity of detection, making it more effective at uncovering anomalous incidents. Despite these benefits, the challenge with entropy-based approaches lies in the computational time and memory usage, particularly in high-speed networks. To address this, researchers have developed optimized algorithms, such as the fast entropy approach, which reduces computation time by calculating the entropy of packet counts more efficiently.

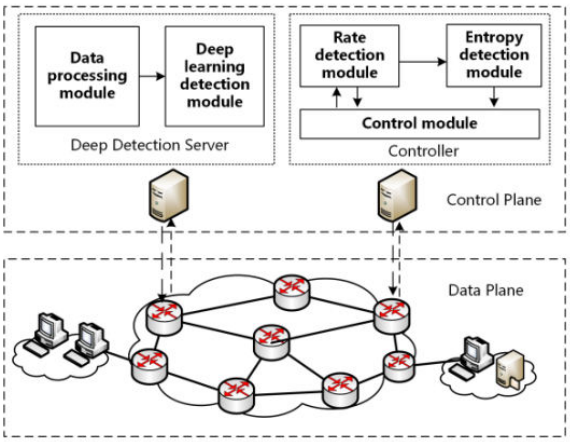

Fig:1.Architecture

III.IMPLEMENTATION

1. Upload DDoS Dataset

In the first step of the implementation, the DDoS dataset is uploaded into the system. This dataset contains network traffic data, including both normal traffic (Benign) and various types of DDoS attacks. The dataset has both numeric and non-numeric values. Since machine learning algorithms can only work with numeric data, the non-numeric data, such as categorical attack types, are converted into numeric form using preprocessing techniques.

2. Preprocess Dataset

Once the dataset is uploaded, it is preprocessed to make it suitable for training machine learning models. During preprocessing, missing values in the dataset are replaced with zeros to handle incomplete data. Additionally, a **Label Encoder** is applied to convert non-numeric features (such as the attack type) into numeric values. After that, the dataset is divided into **training** (80%) and **testing** (20%) sets. The training set is used to train the models, while the test set is reserved for model evaluation.

3. Train Models Using Machine Learning Algorithms

In this step, several machine learning algorithms are trained on the training dataset to learn how to classify network traffic as either benign or an attack. The algorithms used in this project include:

- **Naive Bayes**: A probabilistic classifier based on Bayes' theorem.
- **Random Forest**: An ensemble method that creates multiple decision trees and combines their results.
- **Support Vector Machine (SVM)**: A model that finds the optimal hyperplane to separate attack traffic from normal traffic.
- **XGBoost**: A boosting algorithm that builds a series of decision trees, each improving upon the last.
- **AdaBoost**: Another boosting algorithm that focuses on misclassified data to improve accuracy.
- **K-Nearest Neighbors (KNN)**: A simple algorithm that classifies data based on the majority class of the nearest neighbors.

4. Evaluate Model Performance

After training the models, they are evaluated using the testing dataset. The models' performance is assessed by measuring their prediction accuracy on the test data. This step helps to determine which algorithm performs best for detecting DDoS attacks. The accuracy of each model is calculated, and the model with the highest accuracy is selected for final use.

5. Predict Attacks Using Test Data

In the final step, the trained models are used to predict whether new, unseen test data contains DDoS attack traffic or normal (benign) traffic. The test data, which does not have class labels, is fed into the models, and they predict whether the traffic is an attack or benign. These predictions are then analyzed to verify the model's ability to detect real-time DDoS attacks.

IV.ALGORITHM USED

1. Naive Bayes Algorithm :

The **Naive Bayes** algorithm is a probabilistic classifier based on **Bayes' Theorem**. It calculates the probability of an event (like an attack or normal traffic) occurring, given the evidence (features of the network traffic).

Formula:

Bayes' Theorem is given by:

$$P(A|B) = \frac{P(B|A) \cdot P(A)}{P(B)}$$

Where:

- $P(A|B)$ is the probability of class A (attack or benign) given the observed feature B (network traffic characteristics).
- $P(B|A)$ is the likelihood of observing feature B given class A.
- $P(A)$ is the prior probability of class A.
- $P(B)$ is the probability of observing feature B.

2. Random Forest Algorithm :

The Random Forest algorithm is an ensemble method that builds multiple decision trees and combines their predictions to make a final decision. Each tree is trained on a random subset of the dataset, and the majority vote of all trees is used for classification.

3. Support Vector Machine (SVM)

The **Support Vector Machine (SVM)** is a classification algorithm that finds a hyperplane in a multi-dimensional space that separates the classes (attack and normal traffic) with the maximum margin. This hyperplane is the decision boundary that the SVM uses to classify new data.

Formula:

The decision boundary is defined by the equation:

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

$$w \cdot x + b = 0$$

Where:

- w is the weight vector perpendicular to the hyperplane.
- x is the feature vector of a data point.
- b is the bias term that shifts the hyperplane.

5. AdaBoost Algorithm

AdaBoost (Adaptive Boosting) is another boosting algorithm that focuses on correcting the errors made by previous classifiers. It assigns higher weights to misclassified instances, forcing the model to focus on harder cases.

6. K-Nearest Neighbors (KNN) The **K-Nearest Neighbors (KNN)** algorithm is a simple classification algorithm that assigns a label to a data point based on the majority class of its KKK nearest neighbors in the feature space.

V RESULTS

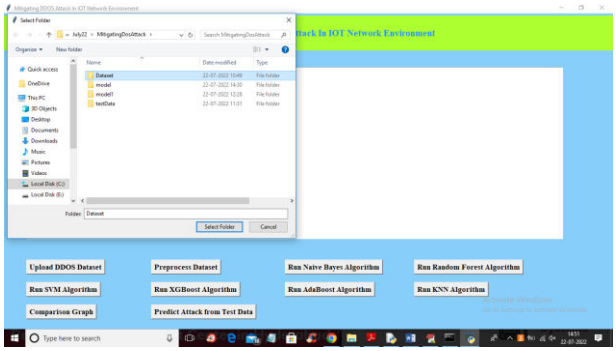

Fig 1: Upload DDOS Dataset

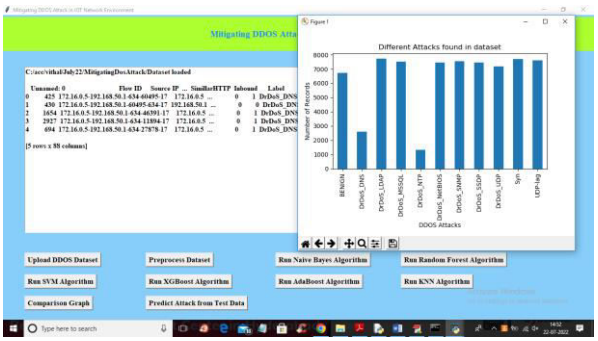

Fig 2: Dataset Loaded and Click on Preprocess Dataset

Fig 3: After Preprocessing Dataset then click on the Run Naive Bayes Algorithm

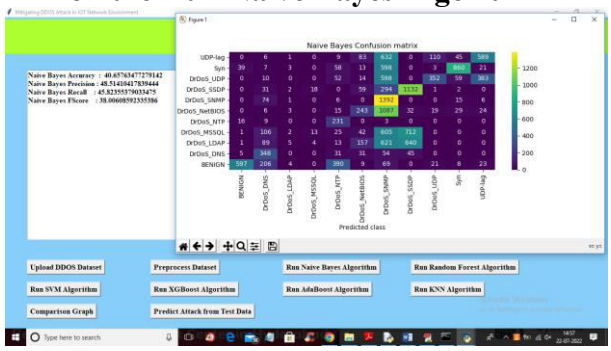

Fig 4 : Naive Bayes predicted then click on 'Run Random Forest Algorithm'

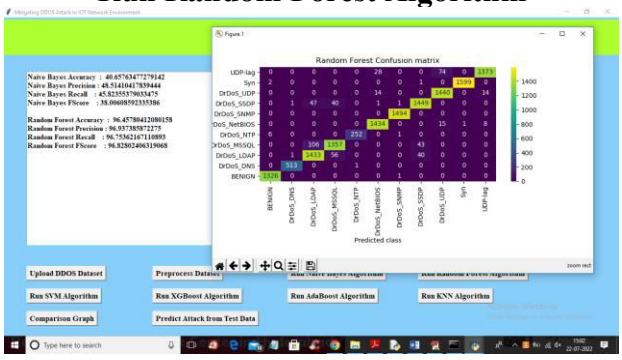

Fig 5 : 'Run SVM Algorithm'

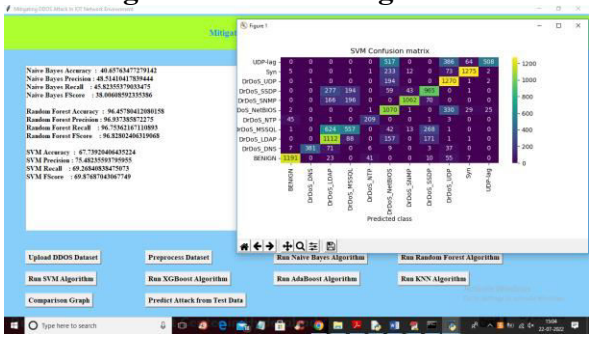

Fig 6 : 'Run XGBOOST Algorithm'

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

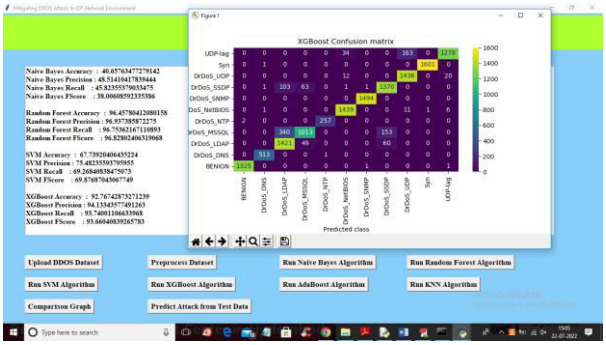

Fig 7: Run ADA BOOST Algorithm

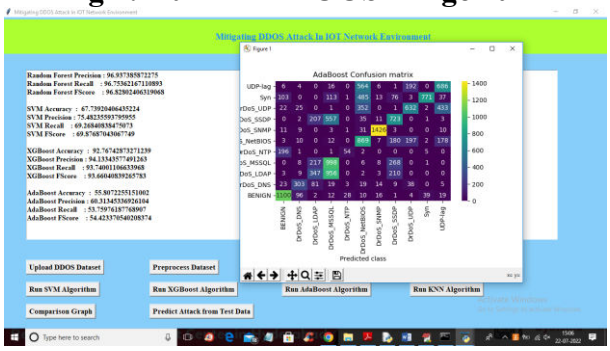

Fig 8 : Run KNN Algorithm

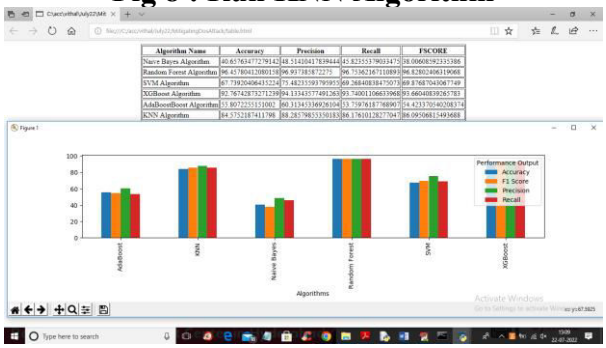

Fig 9: Comparison table

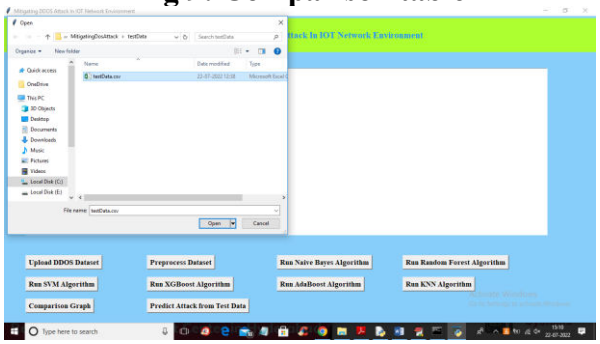

Fig 10: Predict Attack from Test Data

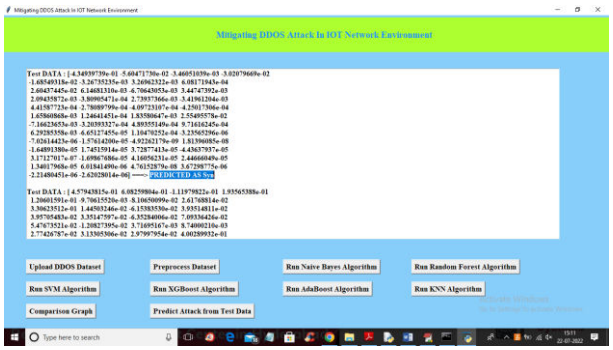

Fig 11: We can see predicted ATTACK as 'SYN'

VI CONCLUSION

We introduced a novel entropy-based approach to detect Distributed Denial of Service (DDoS) attacks, a significant threat to network security. DDoS attacks disrupt the normal functioning of systems by flooding them with excessive traffic, leading to service unavailability. Traditional methods like signature-based detection and anomaly detection often face challenges in recognizing new or zero-day attacks, making it harder to protect critical systems from emerging threats. Our entropy-based method addresses these limitations effectively.Entropy measures the randomness and unpredictability in network traffic patterns. By analyzing entropy values from key traffic features such as packet size, inter-arrival time, and protocol distribution, we can identify anomalies that deviate from the usual patterns of legitimate traffic. These deviations are often indicative of a DDoS attack. Moreover, we enhance the detection process by integrating machine learning algorithms, which help the system learn from historical traffic data, improving the distinction between normal and attack traffic. Our approach was extensively tested on real-world datasets, showing strong performance in detecting DDoS attacks while significantly minimizing false positives. This makes the method not only reliable but also efficient for real-time monitoring and mitigation of threats. The ability to detect attacks early provides a crucial advantage in protecting network

infrastructure, ensuring that critical services remain operational and secure.In conclusion, the proposed entropy-based method offers a promising solution for improving network security by effectively identifying and responding to DDoS attacks. By combining the power of entropy measures and machine learning, we provide a tool that can adapt to evolving attack patterns, making it an essential component of a robust network defense system. Future work could focus on optimizing the approach further, expanding its capabilities, and testing it in more complex network environments to enhance its effectiveness and scalability.

REFERENCES

[1] R. Vishwakarma and A. K. Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoTnetwork", Telecommunication Systems

[2] S. Li, S. Zhao, G. Min, L. Qi and G. Liu, "Lightweight Privacy-Preserving Scheme Using Homomorphic Encryption in Industrial Internet of Things",

[3] S. Li, "Zero Trust based Internet of Things", EAI Endorsed Transactions on Internet of Things,

[4] M. Nooribakhsh and M. Mollamotalebi, "A review on statistical approaches for anomaly detection in DDoS attacks",

[5] N. Agrawal and S. Tapaswi, "Defense mechanisms against DDoS attacks in a cloud computing environment: State-of-the-art and research challenges".

[6] M. A. Alarqan, Z. F. Zaaba and A. Almomani, "Detection mechanisms of DDoS attack in cloud computing environment: A survey", Advances in Cyber Security: First International Conference, August 2019.

[7] L. D. Tsobdjou, S. Pierre and A. Quintero, "An online entropy-based DDoS flooding attack detection system with dynamic threshold"

[8] J. Yuan and K. L. Mills, "Monitoring the macroscopic effect of DDoS flooding attacks"

[9] Y. Chen, K. Hwang and W. S. Ku, "Collaborative detection of DDoS attacks over multiple network domains".

[10] H. Wang, D. Zhang and K. G. Shin, "Change-point monitoring for the detection of DoS attacks"r

[11] S. Oshima, A. Hirakawa, T. Nakashima and T. Sueyoshi, "DoS/DDoS detection scheme using statistical method based on the destination port number", Proceedings of the 2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processig.

[12] İ. Özçelik and R. R. Brooks, "Deceiving entropy based DoS detection", Computers & Security, 2015.

[13] M. H. Bhuyan, D. Bhattacharyya and J. Kalita, "An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection".

[14] Y. Xiang, K. Li and W. Zhou, "Low-rate DDoS attacks detection and traceback by using new information metrics",2011.

[15] I. Basicevic, N. Blazic and S. S Ocovaj, "On the use of generalized entropy formulas in detection of denial of service attacks".

[16] I. Basicevic, N. Blazic and S. Ocovaj, "On the use of principal component analysis in the entropy based detection of denial-of-service attacks", Security and Privacy, 2022.

[17] B. H. Ali, N. Sulaiman and S. Al-Haddad, "Identification of distributed denial of services anomalies by using combination of entropy and sequential probabilities ratio test methods", Sensors, 2021.

[18] M. Zekri, S. E. Kafhali and N. Aboutabit, "DDoS attack detection using machine learning techniques in cloud computing environments", 2017