DETECTION OF DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACK BASED ON FEATURES SIMILARITY AND K-MEANS CLUSTERING

[1]Emmanuel Oluwatobi Asani, [1]Michael N. Moeti [1]Pius Adewale Owolawi
[1]Department of Computer Systems Engineering, Tshwane University of Technology (TUT)
Pretoria, South Africa

ABSTRACT
The detection of distributed denial-of-service (DDoS) attacks is still a difficult subject due to the fact that attackers are constantly coming up with new and creative ways of getting through the security systems that are in existence. The increasing sophistication of Distributed Denial of Service (DDoS) attacks makes identifying them a crucial challenge in network security. The aim of this research is to detect DDoS attacks using a hybrid approach that combines eXtreme Gradient Boosting (XGBoost) and K-means clustering with feature similarities as determined by the Minkowski distance. Rather than relying on the traditional Euclidean distance ($p = 2$), used by K-Means, leading to issues such as sensitivity to the initial cluster centers and the risk of converging on a local minimum, the study integrated the Minkowski distance metric to enhance cluster compactness and flexibility in modeling traffic distributions. The resulting cluster assignments are then integrated as additional features for supervised refinement using XGBoost. Experimental evaluation conducted on the APADDoS dataset showed that the proposed model achieves 90% overall accuracy, 95% precision, 90% recall, and an F1-score of 91% when k = 3 clusters are employed, comparatively outperforming conventional K-Means-based detection models. The results validate that integrating feature similarity measures with gradient boosting enhances detection robustness, reduces false positives, and improves detection capability in practical intrusion detection systems.

Keywords: Distributed denial-of-service (DDoS), unsupervised learning, clustering, supervised refinement, Minkowski distance

1. INTRODUCTION
Today, internet services are essential for both individuals and businesses. With the growth of network-based services, there has been a corresponding rise in network attacks aimed at disrupting these services. Among these, Distributed Denial of Service (DDoS) attacks remain one of the most prominent threats of the internet age. A DDoS attack targets networked resources, such as memory or bandwidth, by overwhelming them with excessive requests until they become unresponsive or unavailable. This attack method exploits the inherent throughput limitations of network resources and their supporting infrastructures [1]. DDoS attacks rely on numerous compromised devices known as “bots” that simultaneously send large volumes of requests to a target system. The attacker, called the botmaster, builds this network of bots, or botnet, by exploiting vulnerabilities in systems, whether due to physical weaknesses or configuration flaws. Trojans and other forms of malware are commonly used to infect these devices. Once enough systems have been compromised, the botmaster launches the attack, flooding the target server or network to incapacitate it [2]. As a result, DDoS attacks pose a significant threat to the availability and performance of online services, often rendering them inaccessible to legitimate users.

Researchers have proposed various solutions, including traffic mining, behavioral analysis, packet-level analysis, flow-level analysis, and deep packet inspection. Both conventional and advanced intrusion detection/prevention systems offer some forms of DDoS protection [3].

However, with attackers adopting increasingly sophisticated techniques, traditional signature-based detection methods have become less effective. This has created the need for more advanced and adaptive detection strategies. In this context, machine learning approaches have gained attention. Several studies have demonstrated the potentials of machine learning techniques in combating DDoS attacks, further strengthening the case for developing more advanced ML-based detection models [3][4]. For example, K-means clustering, a widely used unsupervised learning method, can help detect anomalies in network traffic by grouping data based on feature similarity, potentially exposing abnormal patterns indicative of a DDoS attack. However, K-means has limitations, such as sensitivity to the initial cluster centers, difficulty handling outliers, and the risk of converging on a local minimum [5]. These challenges highlight the need to integrate enhanced feature similarity techniques to improve detection performance. This study therefore presents a DDoS detection model based on features similarity and k-means clustering. The major contributions of this work are:

I. Development of a hybrid approach that combines eXtreme Gradient Boosting (XGBoost) and K-means clustering with feature similarities as determined by the Minkowski distance to identify DDoS attacks.
II. A scalable and adaptable solution that ensures strong network protection while effectively combating the constantly changing DDoS attack scenario.

The rest of this paper is organized as follows. Section 2 reviews related works on the detection of DDoS attacks and the methods used. Section 3 describes the proposed method. Section 4 presents the experimental results obtained using this method. Finally, Section 5 presents a conclusion of the article and recommendations for future work.

2. RELATED WORKS

Addressing the menace of Distributed Denial of Service (DDoS) attacks using traditional run-of-the-mill detection techniques have become increasingly inadequate due to the emergence of novel and sophisticated attack patterns. Consequently, researchers are tending towards exploring robust machine learning and data-driven techniques for automated and adaptive detection. Notably, the integration of advanced feature engineering and parameter tuning offers promising performances in effective DDoS detection. Studies by [6] highlighted that feature engineering niches such as filter, wrapper, as well as hybrid feature selection methods improves the detection of DDoS traffic in machine learning models. Similarly, [7] emphasized that using suitable feature selection methods can potentially improve performance and optimize computational overhead in machine-learning-based DDoS detection models.

Due to its ability to adapt to changing attack patterns and avoid reliance on labeled data, clustering-based unsupervised learning has emerged as a key component of DDoS detection. Clustering methods, especially K-Means, have consequently been explored in the literature for unsupervised or semi-supervised DDoS detection. Clustering models are considered valuable for real time detections due to their internal mechanism of clustering traffic data based on similarity. This mechanism allows normal and anomalous (attack) patterns to emerge without requiring labeled data, thereby yielding high throughput. For instance, [8] modelled a K-Means based ‘semi-supervised’ detection system using the CICIDS2017 dataset. The method included the integration of hybrid feature selection and centroid clustering to obtain optimum centroid which was then used for classification. The approach yielded very promising performance. The study by [9] introduced an enhanced K-Means clustering model in detecting DDoS. The centroid selection module of the K-Means was enhanced by using density and mutual information metrics. This achieved a stable and high detection accuracy (>96%) across

different DDoS variants. Other studies, for instance [10] illustrate the effectiveness of K-Means in partitioning network traffic to detect DDoS behavior, including modified initializations and dynamic windowing to handle large datasets [10].

Recent advances in clustering have shifted focus to the integration feature similarity functions, rather than relying on raw traffic metrics. This idea of measuring similarity among feature vectors has been shown to improve detection accuracy, particularly for low-rate or stealthy DDoS. The study by [11] presents a DDoS detection model, based feature similarity. The transformed feature spaces generated by the feature similarity module enabled enhanced pattern discrimination for improved cluster analysis. This study illustrates the value of similarity measures in clustering-based cyber-attack detection as corroborated in multiple studies reviewed by [12]. The benefits of integrating feature similarity include dimensionality reduction and enhanced discriminative prowess of learning models. Overall, the reviewed studies show that K-Means clustering remains an effective detection technique, particularly when supplemented with careful initialization and feature selection. Furthermore, standalone clustering approaches often suffer from generalization issues, are sensitivity to high dimensionality, and yield performances with high false positives. The integration of adequate feature engineering and similarity measures significantly improves the effectiveness of clustering models in detecting DDoS by emphasizing discriminative traffic characteristics.

3. METHODOLOGY

We present a hybrid DDoS detection framework that integrates feature similarity–based clustering using Minkowski K-Means with supervised refinement via XGBoost. The overall pipeline includes procedures such as data acquisition, preprocessing and feature engineering, similarity-based clustering, supervised classification, and model evaluation. The framework is designed to leverage unsupervised structure discovery while enhancing discriminative performance through gradient boosting. Figure 1 illustrates the procedure flow of the proposed DDoS detection model.

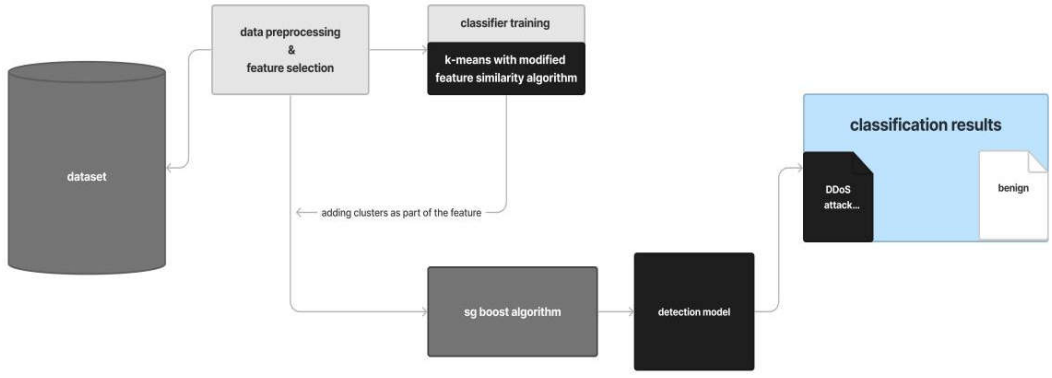

Figure 1. The Architecture of the Proposed model

3.1. Data Collection

The dataset used in this study was obtained from the Kaggle public repository with the url: https://www.kaggle.com/datasets/yashwanthkumbam/apaddos-dataset. The dataset contains 151,201 traffic records and 23 attributes, labeled into three classes as BENIGN, DDoS-PSH-ACK and DDoS-ACK. Since clustering is inherently unsupervised, class labels were removed during the K-Means phase and retained only for supervised refinement and performance evaluation. Categorical attributes (such as source and destination IP addresses) were numerically encoded to enable distance-based computation. Given that the number of record is depicted as n, and number of selected features represented by d, then the processed dataset is defined as:

$$X = \{x_1 x_2, \dots, x_n\}, x_i \in \mathbb{R}^d \qquad (1)$$

3.2. Data preprocessing

In this stage, we include the feature selection and feature standardization approach on the features of the dataset.

3.2.1. Feature Selection

In order to forestall the curse of dimensionality, contain computational overhead and stabilize clustering, six traffic features were selected based on domain knowledge and DDoS behavioral characteristics. They include *Encoded source IP address, Encoded destination IP address, Packet count, IP protocol, Byte count, Flow-related statistical attribute.*

3.2.2. Feature Standardization

The K-Means clustering technique is distance-based, thus feature scaling is essential to standardize the feature coefficients. Consequently, we applied Z-score normalization on the feature set as follows:

$$z_{ij} = \frac{x_{ij} - \mu_j}{\sigma_j} \qquad (2)$$

where:

x_{ij} = original feature value, μ_j = mean of the feature values and σ_j = standard deviation of feature values. This ensures zero mean and unit variance: $\mathbb{E}[z_j] = 0, \mathrm{Var}(z_j) = 1$.

3.3. Model Development

3.3.1. Centroid Computation

The Elbow Method was used to determine the optimal number of clusters k. Given that $C_i =$ cluster i and μ_i is the centroid of cluster i, we compute the Within-Cluster Sum of Squares (WCSS) as follows:

$$WCSS(k) = \sum_{i=1}^{k} \sum_{x \epsilon C_i} ||x - \mu_i||_2^2 \qquad (3)$$

The optimal number of clusters k corresponds to the point where marginal reduction in WCSS diminishes significantly. The elbow method for optimal k is further illustrated in algorithm 1.

Algorithm 1: Elbowpoint heuristic for computing optimal centroid k

Input: Standardized dataset X_r

Output: Optimal number of cluster k^*

1. **For** $k = 1$ **to** k_{max}:
   a. **Fit** k-Means with k clusters
   b. **Compute** $WCSS(k)$
2. **Plot** $WCSS(k)$ vs. k
3. **Select** k^* at the elbow point
4. Return k^*

The resulting plot is presented in Figure 2 showing number of clusters from $k = 1$ to 10. The curve on the graph shows significant change in slope at $k = 2$ with some meaningful improvement at $k = 3$, beyond which the discriminative abilities of the clustering begin to diminish.

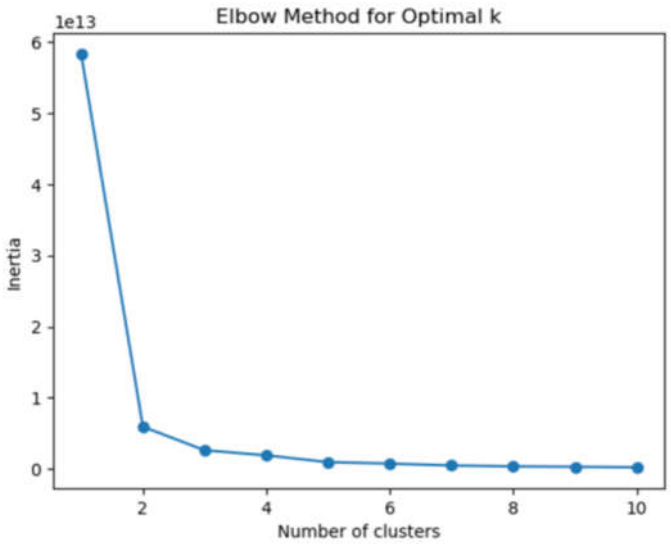

Figure 2. Elbow point method for optimal k

3.4. Modified K-Means clustering with Minkowski Distance

Traditional K-Means uses Euclidean distance ($p = 2$), leading to issues such as sensitivity to the initial cluster centers and the risk of converging on a local minimum. To address this concern, this study generalizes similarity computation using the Minkowski distance:

$$D_p(x, y) = \left(\sum_{j=1}^{m} |x_j - y_j|^p \right)^{\frac{1}{p}} \quad (4)$$

where:
$p \geq 1$;
$p = 1$ gives Manhattan distance
$p = 2$ gives Euclidean distance

This adjustment introduces a flexibility that helps the clustering to better adapt to traffic feature distribution and improve detection accuracy. Thus, the clustering objective becomes:

$$\min_{c} \sum_{i=1}^{k} \sum_{x \epsilon C_i} D_p(x, \mu_i)^p$$

An algorithmic flow of the clustering process based on Minkowski distance is presented in Algorithm 2.

Algorithm 2: Modified K-means algorithm

Input: standardized dataset X_r, number of clustersk^*, distance parameter p
Output: Clustered assignment C

1. Randomize initial centroids $\{\mu_i, \ldots, \mu_k\}$
2. Repeat until convergence
   - Assignment step:
   $$C_i = \{x : D_p(x, \mu_i) \leq D_p(x, \mu_j), \forall j\}$$
   - Update Step:
   $$\mu_i = \frac{1}{|C_i|} \sum_{x \epsilon C_i} x$$
3. Stop when centroid displacement $< \epsilon$

3.5. Supervised refinement using XGBoost

XGBoost (Extreme Gradient Boosting) is an optimized distributed gradient boosting library that is highly efficient, flexible, and portable. After the clustering, supervised refinement was carried out using XGBoost as follows:

Cluster labels were appended to the feature matrix:

$$X_{aug} = [|X_r|C] \tag{5}$$

The augmented dataset was then used to train an XGBoost classifier. Given that $f_k \in \mathcal{F}$ represents a regression tree, while t is the number of trees, then XGBoost builds an additive ensemble model:

$$\hat{y}_i^{(t)} = \sum_{k=1}^{t} f_k(x_i) \tag{6}$$

The objective function is:

$$\mathcal{L}^{(t)} = \sum_{i=1}^{n} l\left(y_i, \hat{y}_i^{(t)}\right) + \sum_{k=1}^{t} \Omega(f_k) \tag{7}$$

with regularization:

$$\Omega(f) = \gamma T + \frac{1}{2}\lambda \sum_{j=1}^{T} w_j^2 \tag{8}$$

Regularization was introduced to prevent overfitting where T = number of leaves; w_j = leaf weight. The XGBoost algorithm is presented in algorithm 3 as follows:

Algorithm 3: XGBoost Training algorithm

Input: Augmented dataset X_{aug}, labels y

Output: Trained ensemble model

1. **Initialize** predictions $\hat{y}^{(0)}$
2. **For** $t = 1$ **to** T:
   a. Compute gradients and Hessians
   b. Fit regression trees to gradients
   c. Update predictions:

$$\hat{\boldsymbol{y}}^{(t)} = \hat{\boldsymbol{y}}^{(t-1)} + \eta \boldsymbol{f_t}(\boldsymbol{x})$$

3. **Return** ensemble $\{f_1, \ldots, f_T\}$

4. Result and Discussion

For the development of the system, an array of tools was used. The experiment was conducted on a Windows system with the following hardware configuration: Processor Intel® Core™ Corei7 with speed 2.60 GHz, RAM of 16GB and a Hard Disk of 256GB SSD. The experiments were designed to evaluate the effectiveness of the proposed Minkowski K-Means + XGBoost hybrid model for DDoS detection.

4.1. Performance Evaluation Metrics

The detection model was evaluated based on metrics such as accuracy, precision, recall and F-measure. Accuracy measures the overall classification correctness of the model as depicted in equation 9.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{9}$$

Recall measures the proportion of actual attacks correctly identified and computed as presented in equation 10.

$$R = \frac{TP}{TP + FN} \qquad (10)$$

Precision is calculated by dividing the number of positive predictions by the proportion of accurate predictions. It measures the proportion of predicted attack instances that are truly attacks.

$$P = \frac{TP}{TP + FP} \qquad (11)$$

F1-measure (F) is referred to as the precision and recall's harmonic average.

$$F = \frac{2 * P * R}{P + R} \qquad (12)$$

Where:
TP (True Positives): Correctly classified positive cases.
TN (True Negatives): Correctly classified negative cases.
FP (False Positives): Incorrectly classified negative cases.
FN (False Negatives): Incorrectly classified positive cases.

4.2 Model Performance and discussion

The model's performance was measured using clustering metric. To achieve this, tests were performed on the model for correctness of results. The performance of the proposed model was evaluated for different values of k (number of clusters) as displayed in Table 1.

Table 1 Showing a table of performance metrics scores

Metric	k=2	k=3
Accuracy	86%	90%
Precision	76%	95%
Recall	71%	90%
F1-score	76%	91%

The results show a significant improvement in the performance of the clustering model when increasing from $k = 2$ to $k = 3$. At $k = 3$, the model achieves an accuracy of 90%, a precision of 95%, a recall of 90% and a F1-score of 91%. The high precision (95%) indicates that the model generates very few false positives, which is critical in DDoS detection to avoid unnecessary mitigation actions. This is further visualized by the confusion matrix chart in Figure 3, which demonstrates strong discriminative capability of the clustering model between benign and attack traffic.

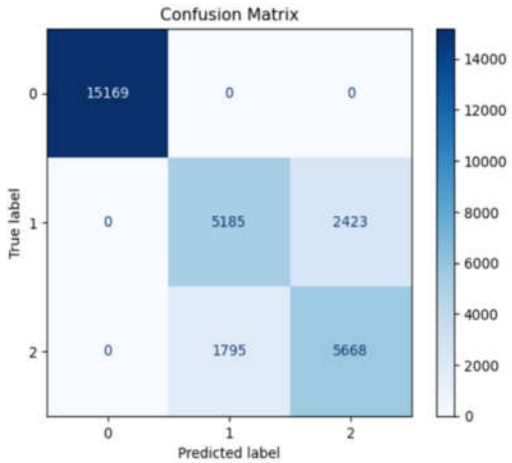

Fig. 3. Confusion matric chart of the proposed model

Figure 4 shows the log-loss curve which confirms stable convergence of the model. The steep decline in log-loss during early epochs indicates that the model quickly captures dominant traffic patterns. Feature representations generated by Minkowski K-Means provide informative structure for XGBoost.

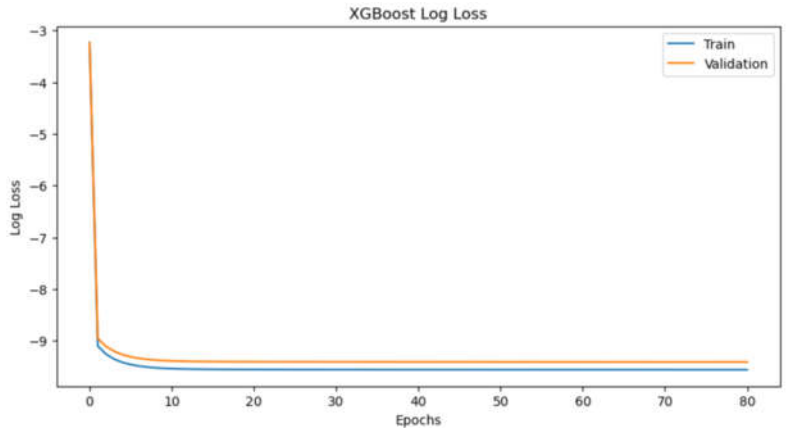

Fig. 4. The log loss chat of the proposed model

The flattening of both curves suggests:

$$\lim_{t \to T} \mathcal{L}_{train}^{(t)} \approx \mathcal{L}_{val}^{(t)}$$

This indicates that additional boosting rounds will not significantly improve performance, as the model has converged. The close overlapping of the training and validation curves shows the effect of the regularization in handing overfitting. Thus the model could be said to have good generalization capability.

To further contextualize the model's capability, it was compared with a similar state-of-the-art by [13] which used augmented K-means clustering approach. Table 2 shows that our approach outperformed [13] by approximately 4% in terms of accuracy, showing relative improvement due to the introduction of the Minkowski distance. The results demonstrate that integrating feature similarity-based clustering with supervised boosting enhances DDoS detection performance.

Table 2. Comparison with existing model related to the study.

Models	Methodology	Accuracy
Proposed model	k-means with Minkowski distance and XGBoost	**90%**
An augmented K-means clustering approach for the detection of distributed denial-of-service attacks [13]	k-means with deep autoencoders	**86%**

Unlike standard Euclidean K-Means, the use of the Minkowski distance metric improves flexibility in modeling feature similarity. This allows better adaptation to the statistical distribution of network traffic features. The improved cluster compactness contributes to higher downstream classification performance. Although the elbow analysis suggested strong separation at $k = 2$, empirical results show that $k = 3$ provides better discriminative power, likely due to finer separation between the two DDoS variants. Furthermore, the incorporation of XGBoost significantly enhanced the predictive capability of the model due to it inherent capability to handling nonlinear relationships between traffic features. XGBoost also minimized residual classification errors from clustering, and eliminated overfitting via regularization. The high precision (95%) indicates strong robustness against false alarms, which is essential in operational network security environments where false positives can disrupt legitimate traffic.

5. CONCLUSON

The study presents a Distributed Denial of Service (DDoS) attacks detection framework based on Minkowski K-Means clustering and supervised refinement with XGBoost. The objective was to enhance predictive capability, accuracy and generalization capability of the model. The experimental evaluation of the model yielded comparatively strong detection performance, with an overall accuracy of 90%, precision of 95%, recall of 90%, and F1-score of 91% at $k = 3$. The confusion matrix analysis demonstrates strong discriminative capability of the clustering model between benign and attack traffic. The incorporation of the Minkowski distance metric enhanced clustering flexibility by allowing adaptive similarity modeling across network traffic features. Unlike conventional Euclidean K-Means, this approach better accommodates variations in traffic distributions. Furthermore, the integration of XGBoost significantly improved classification performance by minimizing residual errors from clustering and applying regularization to prevent overfitting. The log-loss analysis confirmed rapid convergence, stable optimization, and strong generalization without evidence of overfitting. Comparative evaluation showed that the proposed hybrid model outperformed related clustering-based approaches, demonstrating the advantage of combining similarity-based unsupervised learning with gradient boosting techniques. In essence, the study establishes that integrating feature similarity measures with machine learning classifiers provides an effective solution for DDoS detection. Future study may explore adaptive selection of the Minkowski parameter p using optimization techniques.

.

REFERENCES

[1]. Chahal, J. K., Bhandari, A., & Behal, S. (2019). Distributed denial of service attacks: A threat or challenge. New Review of Information Networking, 24(1), 31–103. https://doi.org/10.1080/13614576.2019.1611468

[2]. Hallman, R., Bryan, J., Palavicini, G., Divita, J., & Romero-Mariona, J. (2017). IoDDoS The Internet of Distributed Denial of Service Attacks: A case study of the Mirai malware

and IoT-based botnets. Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES 2017). https://doi.org/10.5220/0006246600470058

[3]. Aamir, M., & Zaidi, S. M. A. (2021). Clustering based semi-supervised machine learning foRDDoS attack classification. *Journal of King Saud University. Computer and Information Sciences/Mağalaẗ Ğam'aẗ Al-malīk Saud : Ùlm Al-ḥasib Wa Al-ma'lumat*, *33*(4), 436–446. https://doi.org/10.1016/j.jksuci.2019.02.003

[4]. Ping Z & Jiao D., (2024). A Study on the Application of Artificial Intelligence in DDoS Attack Defense: A Literature Review Proc. ICBAR '24: 4th International Conference on Big Data, Artificial Intelligence and Risk Management, 200 – 205 https://doi.org/10.1145/3718751.3718783

[5]. Nayini S.E.Y., Geravand S.E. & Maroosi, A., (2017). A novel threshold-based clustering method to solve K-means weaknesses, 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai, India, 2017, pp. 47-52, doi: 10.1109/ICECDS.2017.8389496.

[6]. Liu Z., Wang Y., Feng F., Liu Y., Li Z. &Shan Y (2023). A DDoS Detection Method Based on Feature Engineering and Machine Learning in Software-Defined Networks. *Sensors* 2023, 23(13), 6176; https://doi.org/10.3390/s23136176

[7]. Soim S.S., Sholihin S. & Subianto C.B., (2024). Optimizing Performance Random Forest Algorithm Using Correlation-Based Feature Selection (CFS) Method to Improve Distributed Denial of Service (DDoS) Attack Detection Accuracy *Indonesian Journal of Artificial Intelligence and Data Mining* 7(2):220 DOI: 10.24014/ijaidm.v7i2.24783

[8]. Jasim M.N. & Gaata M.T., (2017). K-Means clustering-based semi-supervised for DDoS attacks classification *Bulletin of Electrical Engineering and Informatics*, 11(6) DOI: https://doi.org/10.11591/eei.v11i6.4353

[9]. Qian H. & Cai L., (2024). Improved K-means-based solution for detecting DDoS attacks in SDN *Physical Communication* 64:102318 https://doi.org/10.1016/j.phycom.2024.102318

[10]. Bagiu S.K., De Carvalho G.C.S., Mishra A., Mink D. Bagiu S.C. & Eager S., (2025). Detecting Cyber Threats in UWF-ZeekDataFall22 Using K-Means Clustering in the Big Data Environment. Future Internet 2025, 17(6), 267; https://doi.org/10.3390/fi17060267

[11]. Sambangi S., Gondi L. & Aljawarneh S., (2022). A Feature Similarity Machine Learning Model for DDoS Attack Detection in Modern Network Environments for Industry 4.0, *Computers and Electrical Engineering* 100:107955 https://doi.org/10.1016/j.compeleceng.2022.107955

[12]. Sudhanva M., Athreya A.P.S., Naveen C.G., Yerriswamy T. & Veena H.N., (2023). Machine Learning Techniques to Detect DDoS Attacks in IoT's, SDN's: A Comprehensive Overview, International Journal of Human Computation and Intelligence 2(4), 203-211

[13]. Marvi, M., Arfeen, A., & Uddin, R. (2021). An augmented K-means clustering approach for the detection of distributed denial-of-service attacks. International Journal of Network Management. 31(3) https://doi.org/10.1002/nem.2160