Implementing Machine Learning (ML) Based Hybrid Model to Mitigate Distributed Denial of Service (DDoS) Attacks in Multi-Access Edge Computing (MEC) Environment

Emmanuel Sibusiso Chaki *, Sekgoari Semaka Mapunya, Mthulisi Velempini

Posted Date: 27 November 2025

doi: 10.20944/preprints202511.2175.v1

Keywords: ML based hybrid model; distributed denial of services attacks; mobile edge computing

 doi:10.20944/preprints202511.2175.v1

Article

Implementing Machine Learning (ML) Based Hybrid Model to Mitigate Distributed Denial of Service (DDoS) Attacks in Multi-Access Edge Computing (MEC) Environment

Emmanuel Sibusiso Chaki *, Sekgoari Semaka Mapunya and Mthulisi Velempini

Department of Computer Science, University of Limpopo, Polokwane, South Africa

* Correspondence: emmzasbu97@gmail.com; Tel.: +27 15 268 2797

Abstract

The fifth-generation mobile network (5G-MN) technology is regarded as an evolution of traditional networks originated from the first, second, third, and fourth generation mobile network respectively. All generational mobile networks are vulnerable to security concerns that are common to traditional mobile communication networks. The security concerns can be hackers compromising the networks by sending malicious packets to authorize user devices which eventually lead to breach of legitimate users' data and also causes high latency in the networks. This security concern evolves with the evolution of communication networks. Therefore, the main objective of this study is to implement a robust mitigation scheme in Mobile Edge Computing (MEC) due to the limitations of traditional approaches in addressing evolving security concerns. MEC is one of the significant technologies in the implementation of 5G-MN. MEC enhances the capabilities of cloud computing and brings computational capability closer to the network edge. This reduces latency in 5G, resulting in better end-user experience. This study focuses on MEC security concerns called distributed denial of service (DDoS) attacks which can occur at different network layers of the network. The aim was to tackle security issues such as DNS flooding attacks and identify effective techniques for mitigating DDoS attacks in MEC systems. We suggested employing Supervised Machine Learning (SML) algorithms as the proposed solution or mitigation techniques, which are Random Forest (RF), Decision Tree (DT), Naïve Bayes (NB), K-Nearest Neighbor (K-NN), Logistics Regression (LR), and Blending/Stacking Model (BM/SM). Subsequently, we then conducted an evaluation of these techniques. The evaluation was based on multiple performance metrics such as accuracy, detection/recall, precision, F1-Measure, Matthew's correlation coefficient (MCC). Machine learning (ML) models were stacked to implement ML-based hybrid model. Our evaluation demonstrated that hybrid models surpassed traditional ML models in performance, with RF being the most effective in mitigating DDoS attacks in MEC. The results were supported by statistical analysis such as Probability Density Function (PDF), Area Under the Receiver Operating Characteristic (AUROC) and hypotheses testing, reinforcing the superiority of hybrid models.

Keywords: ML based hybrid model; distributed denial of services attacks; mobile edge computing

1. Introduction

Out of the five technologies associated with 5G-MN, namely millimeter-wave, Massive multi-user Multiple-Input Multiple-Output (MIMO), Small cell stations, Beamforming, Non-Orthogonal Multiple Access (NOMA), and MEC. MEC is considered crucial technology for cellular communication [1]. MEC extends the capabilities of cloud computing by locating them near the edge of the network. Our study specifically focuses on MEC among the mentioned 5G-MN technologies. In the current era, the society still make use of 4G-MN which can sometimes face limitations of

 doi:10.20944/preprints202511.2175.v1

ultralow latency in certain applications such as real-time gaming or industrial automation (robotics) [2]. In the year 2020, the initial phase of the 5G-MN was deployed and expected to be ten times faster than the fourth-generation mobile network (4G-MN) [3]. 5G-MN is projected to offer higher peak download speeds and more efficient bandwidth utilization when compared to 4G-MN [3]. Additionally, 5G-MN supports a wide array of applications, including cloud systems, augmented reality, industrial automation, mission-critical applications, and self-driving vehicles.

MEC's primary objective is to enhance the efficiency, stability, and integrity of a 5G-MN [1]. Its successful implementation relies heavily on robust security measures, as any vulnerability can lead to compromised end-user experiences. To safeguard against attacks, such as DDoS attacks, security devices are used on enterprise networks to defend against threats from carrier networks. Strengthening security measures not only protects against attacks but also improves the overall quality of network services. As 5G-MN technologies are integrated into application systems, high-security measures are essential to ensure their safety.

DDoS attacks can cause service interruptions, and disruptions rendering the central objective of MEC unrealized [4]. This study is aimed at developing a mitigation strategy to counter DDoS attack effectively. DDoS attacks are characterized by multiple compromised computers working together to target a server, website, or network resource, resulting in disruptions and restricted access for legitimate users. The proposed mitigation scheme aims to address and prevent these disruptive attacks, ensuring the stability and reliability of the MEC system.

Drawing from existing literature recommendations [5,6] et al, we propose the integration of ML techniques (DT, LR, NB, RF) to develop our solution. The purpose of building Stacking hybrid model was to optimize or to improve the mitigation capabilities against DDoS attacks in MEC. The main objective of this research is to develop a hybrid model and assess its performance compared to traditional ML algorithms in mitigating DDoS attacks. The performance of ML models can be affected by the configuration of parameters. Consequently, the SML models implemented with default parameters to avoid biased findings.

This study consists of the two cases. In the first case of the study, we evaluate ML algorithms which are LR, DT, NB, and k-NN, and their performance evaluation based on metrics such as recall, precision, F1-measure, and accuracy. The second case of the study focuses on the evaluation of ML models (DT, NB, and LR) against the proposed Hybrid models. Statistical analysis such as AUROC, PDF of normal distribution, and hypothesis testing are used to evidently support the evaluated findings of the second case of the study.

2. Reviewed Papers

According to paper [7], ML based model was proposed to detect and prevent cyber-attacks on Internet of Things (IoT) networks whereas the focal point of this study is based on mitigating DDoS attacks in MEC environment. The limitation involves that the model's detection performance may vary due to incompetency when applied into big dataset. Therefore, this study utilizes hybrid ML-based which have the capability to perform effectively even when applied to large datasets.

In this paper [8], an ML-driven framework for network intrusion detection was proposed whereas this study proposed hybrid ML-based model for MEC network environment DDoS attacks detection. The evaluation lacks statistical significance testing, preventing definitive claims about model performance differences. Limitation of class imbalance poses challenges to generalizability, as no oversampling techniques were employed. Therefore, this study utilizes statistical metrics (PDF, AUROC, and hypothesis testing) to measure the performance of both traditional and hybrid models. Additionally, random under sampling (RUS) and over sampling (ROS) was utilized to ensure there exists unbiased improvement of effective detection rate.

According to [9], cloud computing has become a significant area of focus for researchers due to its extensive applications and advantages. However, its dependence on the internet for service delivery and its distributed nature present security challenges, particularly the severe threat of insider DDoS attacks that can completely disable services. Conventional defense mechanisms such

 doi:10.20944/preprints202511.2175.v1

as firewalls are ineffective in identifying insider attacks. To address this issue, the paper proposed an anomaly intrusion detection approach within the hypervisor layer, aimed at thwarting DDoS activities between virtual machines.

The proposed intrusion detection employs an evolutionary neural network that combines particle swarm optimization with neural networks for the detection and classification of traffic exchanged between virtual machines. Therefore, our research proposes a hybrid ML model to boost the ability to combat DDoS attacks in MEC. The performance analysis of their proposed intrusion detection demonstrated a success in detecting and classifying the DDoS attacks in the cloud computing environment, with minimal false alarms and high accuracy.

Research in paper [10] introduces a novel mechanism for identifying Low-Rate Denial of Service (LDoS) attack flows in a cloud environment using hypothesis testing. LDoS attack traffic exhibits striking similarities to legitimate traffic, making real-time detection with a low false positive rate challenging. However, the proposed approach, which relies on t-statistic, effectively addresses LDoS attacks. Their findings provide a solid foundation of theoretical and mathematical concepts to substantiate its claims.

To validate the effectiveness of the proposed approach, the researchers conducted numerous experiments using appropriate standard datasets. The results of these experiments demonstrated that the schemes are successful with minimal computing operational overhead. The authors acknowledged that enhancing the efficiency and robustness of the proposed approach can be achieved by incorporating a greater number of parameters for LDoS attack detection. In contrast, they utilized hypothesis testing for identifying the flows of LDoS attack in cloud environment whereas our study uses ML-based hybrid model to detect DDoS attacks in MEC, and thereafter evidently use hypothesis testing to support our findings.

In paper [6], the authors introduced a DDoS detection system employed using both ML and signature-based detection methods. Detecting attacks is a crucial area of investigation in cloud computing, with the aim of ensuring that cloud computing becomes a secure and trustworthy platform for future Internet of Things (IoT) services. The researchers specifically focused on detecting flooding-based attacks that target layer 3 (network layer) and layer 4 (transport layer) in the open system interconnection model which is an application layer model. They employed the DT technique to identify abnormal traffic patterns. A comparative analysis of various ML strategies and algorithms was conducted, leading them to conclude that their proposed approach, using the DT algorithm for DDoS attacks detection, yielded more accurate results compared to other ML algorithms such as NB, and K-NN. Conversely, this study employs an ML-based hybrid approach to mitigate DDoS attacks in the MEC, which is different from their use of ML algorithms, and signature-based detection techniques.

Paper [11] presents a fog computing-based DDoS attack mitigation framework designed to achieve rapid and precise detection. The convergence of 5G and fog computing allows for the effective implementation of security solutions in IoT networks. 5G facilitates the connection of numerous devices with high-speed and low-latency communication capabilities, while fog computing provides the necessary resources (storage and computation) for security measures, including anomaly mitigation.

The framework utilizes an anomaly-based mitigation approach, employing a k-NN classification algorithm in conjunction with a signature database. The database stores previously identified attack signatures, enabling swift detection when a similar attack is launched again. The researchers assessed the effectiveness of the k-NN classifier within the framework using the Canadian institute of cyber security dataset, and the results indicated that the k-NN classifier successfully detects DDoS attacks with high accuracy. Their study is based on fog computing and 5G security issues mitigation, whereas our study focuses on MEC, and 5G security issues.

Paper [12] has introduced a framework that aims to inspect and diagnose DDoS attack traffic. The framework includes a fog defender module, pre-trained with ML algorithms, which assesses incoming data traffic and determines whether it should be forwarded to the cloud server. By

 doi:10.20944/preprints202511.2175.v1

deploying this module within a software defined network (SDN) controller, the framework successfully blocks infected packet IP addresses, allowing only legitimate requests to proceed to the cloud server.

The detection and mitigation of DDoS attacks take place at the network edge through the implementation of SDN, which offers an efficient solution in terms of response time and resource utilization for both fog and cloud environments. Their results demonstrate that the difference in CPU utilization before and after the attack is approximately 13%, indicating that this amount of CPU resources is the overhead required for running the fog defender module. However, this limitation can be mitigated by using high-end machines. The current scheme effectively defends against TCP, UDP, and ICMP attack traffic, and the proposed model performs well with the KNN algorithm, achieving an accuracy of 86%. Our study designed an ML-based hybrid model in MEC to detect DDoS attacks, while their study focused on implementing an ML model to detect DDoS attacks in fog computing.

Authors in [5] initially examines the prediction performance of various ML classification algorithms using a real-time IoT traffic dataset that underwent authentication and validation. The findings demonstrate that LR proves to be the most effective SML classifier, achieving an impressive prediction accuracy of 97% in detecting IoT DDoS attacks. Additionally, the researchers explored the hybridization of LR with optimization algorithms, and the Grasshopper Optimizer Algorithms (GOA) emerged as the most effective in enhancing prediction accuracy to 99%. Consequently, they developed a solution by combining LR with GOA, creating an optimal IoT DDoS attack detection approach.

This study lays the groundwork for a data-driven method to mitigate emerging variants of malicious IoT DDoS attacks, including zero-day attacks. This paper focuses on using ML algorithms for detecting MEC DDoS attacks and designing ML-based hybrid models to enhance the detection capacity whereas their study uses ML to detect IoT DDoS attacks but utilizes GOA to enhance mitigation capacity.

Based on paper [13] a novel approach was introduced in detecting DDoS attacks, combining deep belief network (DBN) feature extraction with the Particle Swarm Optimization and Hybrid Long Short-Term Memory (PSO-LSTM) model. The method primarily focuses on mining IP packet features using DBN and subsequently employs the PSO-LSTM model to predict network traffic and identify DDoS attacks. PSO is utilized to optimize the neural network's weights, ensuring the highest accuracy in classification and prediction. Meanwhile, LSTM is chosen for its ability to retain long-term memory, aiding in superior attack classification.

To evaluate the proposed method's performance, experiments were conducted on the NSL-KDD dataset. The results demonstrated that the proposed approach surpasses all existing DDoS attack prediction systems in terms of accuracy, precision, recall, and F-measure. Moreover, it achieves high accuracy in detecting DDoS attacks, preventing any adverse effects on services in the cloud environment. Both our study and their study investigate DDoS attacks detection in MEC and MCC respectively. However, different hybrid models were utilized, ML-based hybrid model implemented for our study whereas PSO-LSTM model implemented for their study.

3. Simulation Methodology

This paper gives scientific knowledge of the mitigation techniques against DDoS attacks in MEC. Various ML models and the proposed based hybrid-ML model are compared in terms of their effectiveness to detect DDoS attacks in MEC. The simulation tools used to obtain our findings are Python programming language on integrated development environment (IDE) called Jupyter notebook/JupyterLab. The dataset taken from [14] is used to train our ML models and implemented hybrid models.

Domain name system (DNS) refers to the paths through which devices lookup to specific web servers in order to access the internet, whereas DNS flooding attacks refers to flooded traffics of packets to the DNS servers that usually disrupts DNS resolution of that DNS domain. Our study

 doi:10.20944/preprints202511.2175.v1

focuses on DNS flooding attacks, which is a type of a DDoS attack. Different SML techniques were evaluated using performance metrics. The results were derived with the use of Python programming language on JupyterLab. The parameters for the first case, and second case of the study are presented in the following tables. Table 1: Displays the set of parameters configured, and used during the training, and testing of ML models. Table 2: Shows the set of parameters configured, and used during the training, and testing of SML models.

Table 1. First case of the study parameters.

ML Techniques	Parameters
LR	{'C': 1.0, 'class_weight': None, 'dual': False, 'fit_intercept': True, 'intercept_scaling': 1, 'l1_ratio': None, 'max_iter': 100, 'multi_class': 'auto', 'n_jobs': None, 'penalty': 'l2', 'random_state': 888, 'solver': 'lbfgs', 'tol': 0.0001, 'verbose': 0, 'warm_start': False}
DT	{'ccp_alpha': 0.0, 'class_weight': None, 'criterion': 'gini', 'max_depth': None, 'max_features': None, 'max_leaf_nodes': None, 'min_impurity_decrease': 0.0, 'min_samples_leaf': 1, 'min_samples_split': 2, 'min_weight_fraction_leaf': 0.0, 'random_state': None, 'splitter': 'best'}
NB	{'priors': None, 'var_smoothing': 1e-09}
KNN	{'algorithm': 'auto', 'leaf_size': 30, 'metric': 'minkowski', 'metric_params': None, 'n_jobs': None, 'n_neighbors': 1, 'p': 2, 'weights': 'uniform'}

Table 2. Second case of the study parameters.

SML Techniques	Parameters
DT	{'ccp_alpha': 0.0, 'class_weight': None, 'criterion': 'gini', 'max_depth': 5, 'max_features': None, 'max_leaf_nodes': None, 'min_impurity_decrease': 0.0, 'min_samples_leaf': 1, 'min_samples_split': 2, 'min_weight_fraction_leaf': 0.0, 'random_state': None, 'splitter': 'best'}
NB	{'priors': None, 'var_smoothing': 1e-09}

 doi:10.20944/preprints202511.2175.v1

LR	{'C': 1.0, 'class_weight': None, 'dual': False, 'fit_intercept': True, 'intercept_scaling': 1, 'l1_ratio': None, 'max_iter': 100, 'multi_class': 'auto', 'n_jobs': None, 'penalty': 'l2', 'random_state': 5, 'solver': 'lbfgs', 'tol': 0.0001, 'verbose': 0, 'warm_start': False}
RF	{'bootstrap': True, 'ccp_alpha': 0.0, 'class_weight': None, 'criterion': 'gini', 'max_depth': None, 'max_features': 'auto', 'max_leaf_nodes': None, 'max_samples': None, 'min_impurity_decrease': 0.0, 'min_samples_leaf': 1, 'min_samples_split': 2, 'min_weight_fraction_leaf': 0.0, 'n_estimators': 10, 'n_jobs': None, 'oob_score': False, 'random_state': None, 'verbose': 0, 'warm_start': False}
Stacking/Blending	Include all the parameters of the ML models (DT, NB, LR, and RF), which are mentioned in this very same Table 2.

Both of the Table 1, and Table 2 entail the configured parameters of the proposed SML techniques used to deal with DNS flooding attacks in terms of detection rates. Table 1 is based on the first case of the study proposed traditional ML techniques (LR, DT, NB, and KNN). Table 2 is based on the second case of the study of traditional SML techniques (DT, NB, LR, and RF) used to implement hybrid model (Blending model).

The system requirements used to perform our experiments are divided into two categories namely, hardware specifications which consists of Processor – i5 (11th Gen Intel(R) Core (TM) i5-1135G7 @ 2.40GHz 2.42 GHz), Random access memory (RAM) – 8.00 GB, System Free Space – Minimum 15GB, System type – 64-bit operating system: x64-based processor, and software specification which consists of IDE (JupyterLab or Jupyter notebook), and Python programming language

4. Results and Data Analysis

The initial instance of experimental results in the study was obtained by utilizing a DNS flooding attacks dataset, where 70% was used for training, and 30% was used for testing. The collected data was not balanced, and we balanced it using random under sampling (RUS) techniques. We computed the performance metrics (recall, precision, F1-measure, and accuracy) for ML models (LR, DT, NB, and K-NN) to evaluate their effectiveness in detecting DNS flooding in MEC. Figure 1 presents the computed findings for each ML model.

Figure 1 presents the computed metric outcomes for each ML algorithm. Based on our findings we can observe from Figure 1 that all ML models achieved the highest accuracy score of 100% except K-NN which is 99%. Data exploratory analysis was well performed to avoid biased building of SML models. KNN couldn't reached 100% due to underfitting of the dataset because RUS was used to balance the dataset. In that case we can conclude that each model can detect DNS flooding attacks network activities in MEC with good precision.

When the ML model exhibits low recall and high precision, it indicates a bias towards DDoS attack detection. Therefore, the F1-measure should be compared to making a final decision on determining the best model. The NB model achieved a 70% recall score and a 76% precision score,

 doi:10.20944/preprints202511.2175.v1

which implies a bias towards detecting either benign or DNS flooding attacks network activities. KNN exhibits no bias in identifying network activities (benign or DNS flooding attacks). However, its lowest F1-measure score of 70% indicates that the model is outperformed by NB which achieved 72% F1-measure score. LR, DT, and K-NN are not biased. As the F1-measure score increases, the level of optimality in detecting DDoS attacks also increases. However, the order of ML models from least optimal to most optimal can be arranged as follows: LR, DT, NB, and K-NN, respectively.

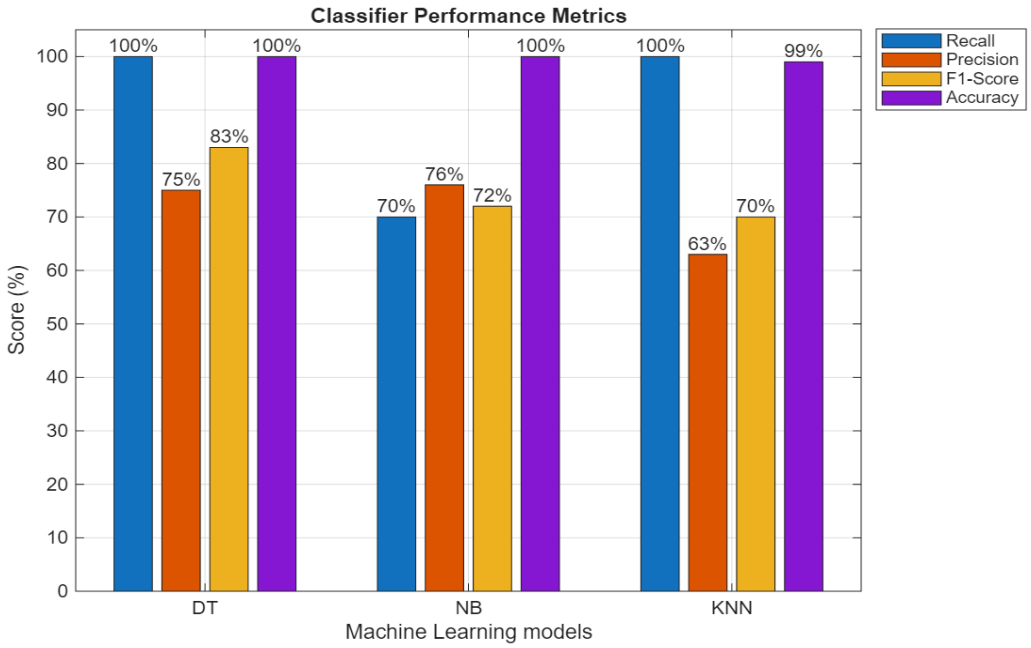

Figure 1. ML Models Results.

In the second case of the study the experimental results were computed based on the splitted dataset, 20% test and 80% training data. The same dataset from the first case of the study was utilized but synthetically generated to make the problem more difficult to deal with. Creating a hybrid model such as blending involves the construction of ML models that will be stacked together to design it. Figure 2 below presents the process of implementing the Stacking model.

Figure 2 shows stacking ensemble architecture which involves combining predictions from several base model learners and meta-learners to create an improved predictive model. A Blending algorithm takes input from individual sub-models and strives to merge them into a superior prediction by learning the optimal way to combine their outputs. This process is also referred to as stacked generalization. The stacking model's design involves incorporating two or more base or learner models, alongside a meta-model responsible for amalgamating predictions generated by these base models.

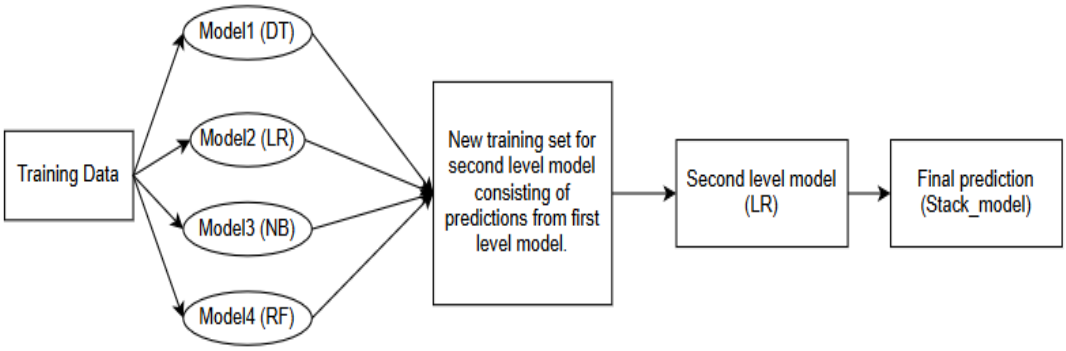

Figure 2. Stacking model process.

 doi:10.20944/preprints202511.2175.v1

ML models such as DT, LR, NB, and RF are stacked to implement ML-based hybrid model. The results obtained from the base models (ML models such as DT, LR, NB, and RF) are referred to as level 0 predictions, LR is regarded as meta model. While the stacking model results are termed level 1 predictions.

Figure 3 below displays the outcomes of our implemented hybrid models (RF and Stacking hybrid model) as well as our ML models (DT, LR, and NB).

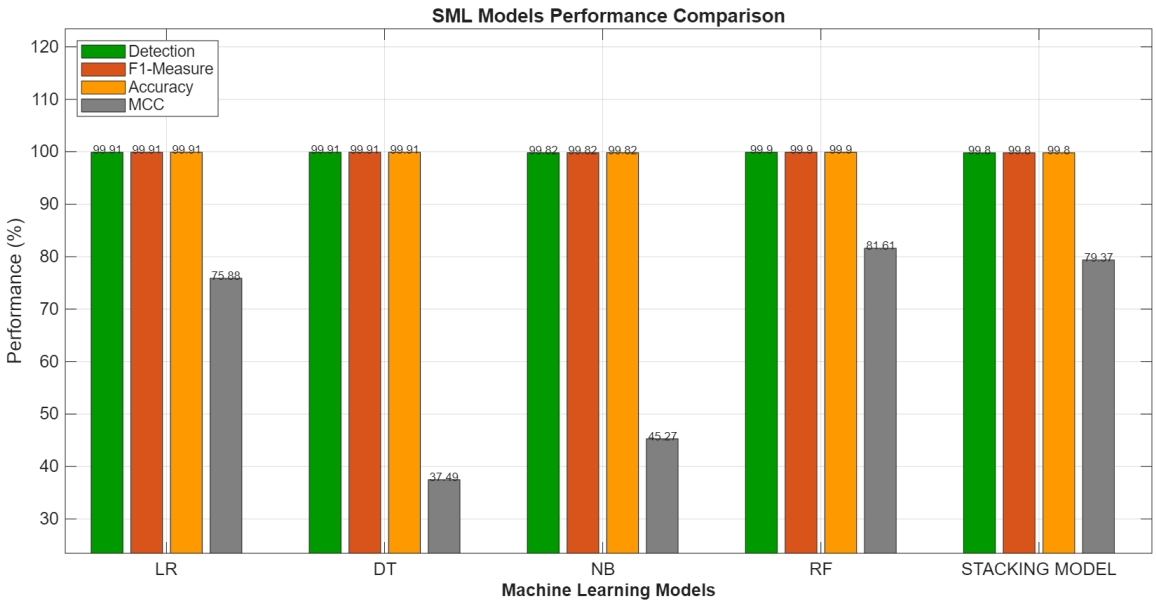

Figure 3. SML Models Results.

Figure 3 demonstrates the comparison results of ML-based hybrid and ML models in accurately identifying the network activities in MEC. All SML models achieved impressive scores of at least 98% for key metrics, including accuracy, F1-measure, and detection. However, there is a slight difference in the F1-measure scores. Based on the first case study analysis, F1-measure scores are useful for assessing the performance of ML models. Likewise, in this study, the effectiveness of each SML model is measured using the F1-measure metric.

Hybrid models outperformed the ML models by achieving the highest F1-measure scores. This implies that ML-based hybrid models are the best compared to ML models in detecting the DDoS attacks in MEC: Hybrid models: first (1st)-Stack model = 99.94%, and second (2nd)-RF = 99.91%. ML models: third (3rd)-LR = 99.89%, fourth (4th)-NB = 99.80%, and fifth (5th)-DT = 99.43%. When comparing MCC scores, there is a competition of hybrid models, as RF outperforms stack model by 2.24%. When comparing the MCC scores, there is a rivalry between the hybrid models, with the RF model outperforming the Stack model by 2.24%.

To further validate our evaluated findings, statistical measurements were utilized. This includes statistical techniques such as AUROC, PDF of the normal distribution, and hypothesis testing, were utilized to robustly validate our findings in both the initial and subsequent stages of the study. The evaluation of these PDFs, AUROC score, and hypothesis testing provide clear and solid support for our conclusions.

PDF of normal distribution, and AUROC findings were based on the synthetic dataset that we re-generated using the collected DNS flooding attack data. Subsequently, we divided the data into training and testing sets, with proportions of 80% and 20%, respectively. Several classification models, including the DT, KNN, NB, LR, RF-hybrid model, and Stacking/Blending-hybrid model, were built.

To assess the performance of each model, AUROC scores were computed, and PDFs curves are presented. Both AUROC scores, and PDF of normal distribution curves were used to evaluate and

 doi:10.20944/preprints202511.2175.v1

compare the effectiveness of each classification model. ROC curves are presented in Figure 4, 5, and 6. PDF of normal distribution curves are presented in Figure 7

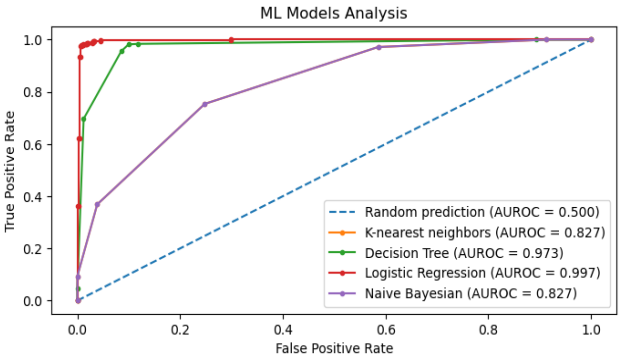

Figure 4. ML Models AUROC Analysis.

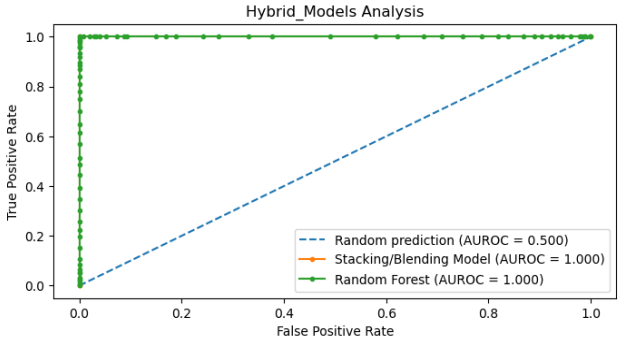

Figure 5. ML-based hybrid Models AUROC Analysis.

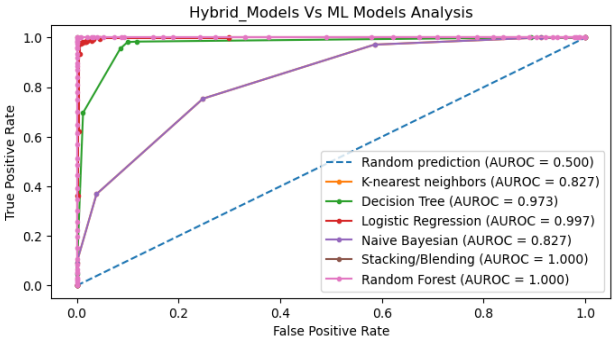

Figure 6. ML vs ML-based hybrid Models AUROC Analysis.

The model with a ROC curve line lying under the diagonal line exhibits that the performance of diagnostic test completely unsuccessful. Based on a rough classification [15], in general, AUC is interpreted as follows: 90% -100% = excellent; 80% - 90% = good; 70% - 80% = fair; 60% - 70% = poor; 50% - 60% = fail.

Figure 4 demonstrates ML models comparison with the use of AUROC scores. LR models achieved excellent AUROC score of 99.7%, which implies that LR outperformed other ML models: DT, NB, and KNN, respectively. However, all ML models achieved at least good to go AUROC scores. Figure 4 shows ML models AUROC analysis performance which ranges from LR, DT, NB, and K-NN respectively, this precisely concurs the first case of the study findings.

Figure 5 evidently shows that all ML-based hybrid models are quite excellent in performance.

 doi:10.20944/preprints202511.2175.v1

Figure 6 shows the comparison of ML against ML-based hybrid models, wherein all hybrid models achieved an excellent AUROC score of 100%, which clearly outperformed all ML models.

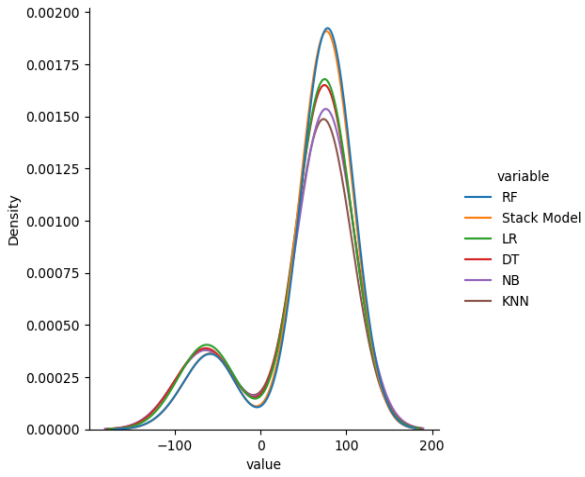

Figure 7. ML vs ML-based hybrid Models PDF of normal distribution.

A PDF of normal distributions pertains to continuous random variables and presents the computed probabilities associated with ranges of values rather than individual values. This is because, in the context of continuous random variables, the probability of any single value is effectively zero. The PDF presented for Normal distribution is derived from detecting rate scores obtained in the first and second case of the study. Separate data-frames were created for each SML technique, containing their respective range of detection or recall scores.

Based on Figure 7, the probability of detection for every SML model is at a minimum of $(P(X = x) = 0.00150)$. It is evident from the calculated probabilities for each SML model that as the random variables approach 100%, the likelihood of high probability detections by the model increases. This suggests the indication that a higher probability of detection implies the model's effectiveness in identifying DDoS attacks. Probability detections of RF and Stacking hybrid model are approaching $(P(X = x) = 0.002)$, whereas LR, and DT approaches $(P(X = x) = 0.00175)$.

Figure 7 shows ML models PDF analysis performance which ranges from LR, DT, NB, and K-NN respectively, this precisely concurs with the first case of the study findings. Figure 7 also shows comparison of ML against the ML-based hybrid model. However, Hybrid models achieved high probability detections compared to ML models which evidently supports the second case of the study that ML-based hybrid models outperformed ML models.

This research study concludes the evaluated results using hypothesis testing. Based on the outcomes obtained, a research hypothesis question was formulated. In hypothesis testing, certain principles must be followed. If the sample size is equal to or greater than 30, the Z-test statistic (z_t) for the population proportion should be used, and a normal distribution must be assumed. The formulated question is as follows:

Author 1 asserts that the ML-based hybrid models, namely the Stacking model and RF, indeed achieved an F1-measure score of at least 90%. On the other hand, author 2 claims that both the Stacking model and RF achieved an F1-measure score of at most 90%. To test this, a random sample of 1406 out of 3812 network activities (including either benign or DNS DDoS attacks) was taken at a 95% confidence interval

Step 1: Our null hypothesis is assumed to be true, until proven contrary.

$\boldsymbol{H_0}$: F1-measure score ≤ 90% (The hybrid models achieve F1-Measure score of less than or equal to 90%).

$\boldsymbol{Ha}$: F1-measure score > 90% (The hybrid models achieve F1-Measure score greater than 90%).

Step 2: Computing significance level.

 doi:10.20944/preprints202511.2175.v1

$$\alpha = 1 - C = 1 - 0.95 = 0.05$$

Step 3: The test statistic for this problem is sample proportion which is the number of network activities that are correctly classified by ML-based hybrid model divided by the total number of network activities sampled. Let P_0 be the true proportion of correctly classified network activities by the ML-based hybrid model.

Computing sample proportion mean:

$$\hat{p} = \frac{X}{n} = \hat{p} = \frac{1406}{3812} = 0.37$$

Computing Z-test statistic (z_t) for population proportion

$$z_t = \frac{\hat{p} - P_0}{\sqrt{\frac{p_0(1 - P_0)}{n}}} = \frac{0.37 - 0.90}{\sqrt{\frac{0.90(1 - 0.90)}{3812}}} = -109.08$$

Step 4: The rejection zone is the range of test statistic values for which we reject the null hypothesis. Given that this is a one-tailed test with a significance level of 0.05, we reject the null hypothesis if the test statistic is smaller than the critical value zα = -1.645. Since our test statistic $Z_t = -109.08$ is smaller than the critical value $z_a = -1.645$, we reject the null hypothesis. Therefore, we have sufficient evidence to support the claim made by Author 1 that the ML-based hybrid models indeed achieved at-least 90% of F1-measure score.

4. Discussion, Conclusions & Recommendations

ML-based hybrid models (RF, and Stacking/Blending model) were implemented to enhance the mitigation capabilities of DDoS attacks in MEC. These models were used to classify over a thousand records. The first case of the study evaluated finding demonstrates that LR outperformed DT, NB, and KNN respectively. Their performance was based in terms of detecting DDoS attacks in MEC.

The empirical statistical methods such as AUROC scores, ROC curves, and PDF of normal distribution precisely arrive at the same results as the simulation results. The second case of the study evaluations demonstrated that ML-based hybrid models outperformed ML models (LR, DT, NB, and K-NN). Statistical methods such as ROC curves, PDF of normal distribution, and hypothesis testing substantiate our evaluated findings. Hence, we can conclude that our study involves no drawbacks since we successfully or evidently supported our simulation findings.

In the future, it is essential to conduct research based on applying unsupervised or semi-supervised learning techniques within a cloud environment dataset such as fog computing or MEC in 5G-MN technologies such as MIMO, NOMA, small cell station, or beamforming. This examination will provide more tangible insights, and scientific knowledge into how ML paradigms perform and how suitable it is for real-world situations.

Abbreviations

The following abbreviations are used in this manuscript:

ML	Machine Learning
SML	Supervised Machine Learning
MCC	Mobile edge computing
5G-MN	Firth-generation mobile network
4G-MN	Fourth-generation mobile network
MEC	Multi-access edge network
SDN	Software defined network
DDoS	Distributed denial of service attacks
DT	Decision Tree
RF	Random Forest
K-NN	K-Nearest Neighbor
LR	Logistic Regression
BM/SM	Blending/Stacking hybrid model
PDF	Probability density function

 doi:10.20944/preprints202511.2175.v1

AUROC	Area under receiver operating characteristics
MIMO	Multiple input multiple output
NOMA	Non-orthogonal multiple access
DBN	Deep belief network
IDE	Integrated development environment
RAM	Random access memory

References

1. J. Nakazato, L. Zongdian , M. Kazuki , K. Keiichi , Y. Tao , K. T. Gia , S. Kei and M. Soh , "Mec/cloud orchestrator to facilitate private/local beyond 5g with mec and proof-of-concept implementation," *Sensors 22 no. 14,* p. p.5145, 2022.
2. D. Chmieliauskas and P. ŠArūNas , "Evaluation of Uplink Video Streaming QoE in 4G and 5G Cellular Networks Using Real-World Measurements," *IEEE Access* , 24 March 2025.
3. Bangalore and M. P. Delhi, "LANDSCAPE ON 5G TECHNOLOGY ATechnology AND SERVICE PROVIDERS PERSPECTIVE," 2020.
4. Osanaiye and A. Opeyemi, "DDoS defence for service availability in cloud computing," 2016.
5. T. Farid and S. Maheyzah, "Hybrid of Supervised Learning and Optimization Algorithm for Optimal Detection of IoT Distributed Denial of Service Attacks," *International Journal of Innovative Computing, 13(1),* pp. 1-12, 2023.
6. M. Zekri, E. K. Said , A. Noureddine and S. Youssef, "DDoS attack detection using machine learning techniques in cloud computing environments," *In 2017 3rd international conference of cloud computing technologies and applications (CloudTech),* pp. 1-7. IEEE, 2017.
7. A. Alomiri, M. Shailendra and A. Mohammed , "Machine learning-based security mechanism to detect and prevent cyber-attack in IoT networks," *International Journal of Computing and Digital Systems 16.1,* pp. 645-659, Aug 2024.
8. J. Khan, E. Rana , S. Hiba , P. Mahira , S. Emaan , D. Salam and A. Fadi , "Can Machine Learning Enhance Intrusion Detection to Safeguard Smart City Networks from Multi-Step Cyberattacks?," *Smart Cities 8, no. 1,* p. p.13, January 2025.
9. A. Rawashdeh, A. Mouhammd and A.-H. Muna, "An anomaly-based approach for DDoS attack detection in cloud environment," *International Journal of Computer Applications in Technology, 57(4),* pp. 312-324, 2018.
10. K. Bhushan and B. B. Gupta, "Hypothesis test for low-rate DDoS attack detection in cloud computing environment," *Procedia computer science 132,* pp. 947-955, 2018.
11. M. A. Lawal, A. S. Riaz and R. H. Syed, "A DDoS attack mitigation framework for IoT networks using fog computing," *Procedia Computer Science 182,* pp. 13-20, 2021.
12. R. Priyadarshini, K. B. Rabindra and D. Harishchandra, "Fog-SDN: A light mitigation scheme for DdoS attack in fog computing framework," *International Journal of Communication Systems 33(9),* p. e4389, 2020.
13. A. Thangasamy, S. Bose and G. Logeswari, "A Novel Framework for DDoS Attacks Detection Using Hybrid LSTM Techniques," *Computer Systems Science & Engineering 45 no. 3,* 2023.
14. C. I. f. Cybersecurity, "DDoS Evaluation Dataset (CIC-DDoS2019)," 2019. [Online].
15. Safari, Saeed, N. Ahmed, B. Alireza and E. Mohamed, "Evidence based emergency medicine; part 5 receiver operating curve and area under the curve," *Emergency 4(2),* p. 111, 2016.
16. H. Rutvij, J. P. Jhaveri and C. J. Devesh, "DoS Attacks in Mobile Ad Hoc Networks: A Survey," pp. pp. 535-541, 7 Januaey 2012.
17. S. M. Ana, P. Zeeshan, A. C. Jose and M. K. Asad, "Towards the transversal detection of DDoS network attacks in 5G multi-tenant overlay networks," *Computers & Security,* vol. 29, pp. 132-147, 2018.
18. Deepali and B. Kriti, "DDoS attack defense framework for cloud using fog computing," in *2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Bangalore, India, 2018.
19. G. GÜRKAN, K. ANSHUMAN, D. A. CHAMITHA, P. QUOC-VIET, N. KHAC-HOANG, L. MADHUSANKA and P. PAWANI, "Integration of ICN and MEC in 5G and Beyond Networks: Mutual Benefits, Use Cases, Challenges, Standardization, and Future Research," *IEEE Open Journal of the Communications Society,* pp. 1382 - 1412, 2022.

 doi:10.20944/preprints202511.2175.v1

20. L. Jingsen, M. Yinan, L. Xiaozhen and L. Yu, "A dynamic adaptive firefly algorithm with globally orientation," *Mathematics and Computers in Simulation,* vol. 174, pp. 76-101, 2020.
21. O. Jude and L. I. A. a. M. Y. Madhusanka, "Cloud and MEC security. A Comprehensive Guide to 5G Security," in *A Comprehensive Guide to 5G Security*, books.google.com, 2018, pp. 373-397.
22. X. Liang, W. Xiaoyue, D. Canhuang, D. Xiaojiang, C. Xiang and G. Mohsen, "Security in mobile edge caching with reinforcement learning," *IEEE Wireless Communications,* vol. 25, no. 3, pp. 116-122, 2018.
23. Mishra, Anupama, B. Brij, Gupta, P. Dragan, J. G. P. Francisco and H. Ching-Hsien, "Classification Based Machine Learning for Detection of DDoS attack in Cloud Computing.," in *In 2021 IEEE International Conference on Consumer Electronics (ICCE), pp. 1-4. IEEE*, 2021.
24. A. L. Muhammad, A. S. Riaz and R. H. Syed, "A DDoS Attack Mitigation Framework for IoT Networks using Fog Computing," *Procedia Computer Science,* vol. 182, no. 2021, pp. 13-20, 2021.
25. D. Nhu-Ngoc, P. Trung, S. Umar, K. Joongheon, B. Thomas, D. Dinh-Thuan and C. Sungrae, "Securing heterogeneous iot with intelligent ddos attack behavior learning," *IEEE Systems Journal,* pp. 1-10, 2021.
26. A. O. Opeyemi, D. Mqlhele and R. C. Kim-Kwang, "DDoS defence for service availability in cloud computing," University of Cape town, Cape town, 2016.
27. H. Qiang, W. Cheng, C. Guangming, L. Bo, Z. Rui, Z. Qingguo, X. Yang, J. Hai and Y. Yun, "A Game-Theoretical Approach for MitigatingEdge DDoS Attack," *IEEE Transactions on Dependable and Secure Computing,* no. 1, p. 1, 2021.
28. D. Ramraj, L. Praveen, C. Gaurav, Y. Ilsun and P. Giovanni, "Study and Investigation on 5G Technology: A Systematic Review," *Advanced Wireless Sensing Techniques for Communication,* vol. 22, no. 1, p. 26, 2022.
29. S. Thulitha, S. Zujany, H. L. Vinh, M. Samuel, S. Bartlomiej, L. Madhusanka and W. Shen, "A Survey on XAI for Beyond 5G Security: Technical Aspects, Use Cases, Challenges and Research Directions," *Networking and Internet Architecture,* 2022.
30. N. TOMASZ, S. MARIUSZ, K. ZBIGNIEW, N. WOJCIECH, A. RAFAL, B. KRZYSZTOF, O. TOMASZ and W. JEAN-PHILIPPE, "Verticals in 5G MEC-Use Cases and Security Challenges," *IEEE ACCESS,* pp. 87251-87298, 2021.
31. B. Xiaoming, T. Wenan and X. Ruohui, "A DDoS-oriented Distributed defense framework based on edge router feedbacks in Autonomous Systems," in *International Multi-symposiums on Computer and Computational Sciences*, Shanghai, China, 2009.