INTERNATIONAL JOURNAL OF SOFTWARE ENGINEERING AND COMPUTER SYSTEMS
E-ISSN: 2180-0650
VOLUME 10, ISSUE 1, 2024, pp. 50 – 59
DOI: https://doi.org/10.15282/ijsecs.10.1.2024.5.0123

RESEARCH ARTICLE

A Novel Approach for Addressing IoT Networks Vulnerabilities in Detection and Classification of DoS/DDoS Attacks.

Aisha Ibrahim Gide*, Abubakar Aminu Mu'azu

Faculty of Natural and Applied Sciences, Umaru Musa Yar'adua University, 820102 Katsina State, Nigeria.

ABSTRACT - The substantial growth of Internet-connected devices within the Internet of Things (IoT) has given rise to significant security challenges. Among the various threats confronting these interconnected devices, Denial of Service (DoS)/Distributed Denial of Service (DDoS) attacks emerge as significant concerns. The attacks, which seek to disrupt IoT services by flooding networks with unnecessary traffic, there is a critical need for robust security measures. Intrusion Detection Systems (IDS) are vital in identifying suspicious activities, yet many existing systems lack real-time capabilities to address evolving attack strategies. This study investigates the vulnerabilities of IoT networks and the pressing need to detect and classify DoS/DDoS attacks in real time. Traditional IDS, while effective in recognizing known attack patterns, fall short in identifying new attack types due to their reliance on historical data. To bridge this gap, this research focuses on developing an enhanced hybrid network intrusion detection and classification system. This study seeks to make contribution to the advancement of resilient security measures within IoT environments. The framework uses the Kth Nearest Neighbor (KNN) algorithm and dense neural networks to efficiently detect and categorize DoS/DDoS attacks in real time. To achieve this, a simulation model implementing the proposed hybrid algorithm will be developed. The framework utilized the MQTT-IoT-IDS2020 dataset, and a comparison was presented with recent approaches found in the literature. The results demonstrated enhanced performance in terms of true positive rate, accuracy, speed of detection.

ARTICLE HISTORY
Received : 18 March 2024
Revised : 13 August 2024
Accepted : 26 September 2024
Published : 2 October 2024

KEYWORDS
IoT security
Real-time DDoS detection
Kth Nearest Neighbor (KNN)
Dense neural networks

1.0 INTRODUCTION

The term Internet of Things (IoT) describes a system in which physical objects, equipped with sensors, software, and diverse technologies, engage in interactions and exchange data with other devices and systems through the internet. Although IoT has streamlined the management of everyday tasks, it is crucial to ensure that criminals cannot exploit vulnerabilities to gain unauthorized access to our homes. As systems advance and incorporate smart security features, hackers also enhance their techniques. IoT devices accumulate substantial data throughout their lifespan. The swift integration of 5G technology is expected to significantly amplify data communication between devices and networks. It's important to emphasize that if the data collected or generated by these devices is not adequately secured, it becomes susceptible to theft for financial motives or, more alarmingly, could jeopardize the lives of people globally [1]. Over time, the number of interconnected devices in the Internet has been steadily increasing, with projections indicating a significant surge in their quantity in the coming years. Coined by Kevin Ashton in 1999, IoT embodies a network enabling billions of devices to communicate and connect concurrently. This type of network does not require expensive components but can be constructed using cheap sensors and interconnected objects. These devices gather information from the environment, facilitating enhancements in our lifestyle [2].

Nowadays, the rapid and extensive development of IoT devices brings forth many challenges and security issues that require attention. Given the widespread presence of these devices in various aspects of our lives, coupled with their role in collecting information about our daily activities, they become susceptible to various types of attacks. As a result, it is crucial to have systems and solutions in place to detect and mitigate these security challenges and issues. The high level of connectivity in the IoT environment exposes constrained devices to external threats, including replay attacks, man-in-the-middle attacks, Distributed Denial of Service (DoS), amplification attacks, flooding attacks, and more. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks have become particularly prevalent in recent years, and they can be launched through various methods [3].

The significance of DDoS (Distributed Denial of Service) attacks on IoT (Internet of Things) devices lies in the rapid development of these devices and their inherent security vulnerabilities. With an estimated 14.4 billion IoT devices globally in 2023, expected to grow to 25.4 billion by 2030, the attack surface for cybercriminals has expanded.

***CORRESPONDING AUTHOR | A.I Gide** | ✉ aisha.ibrahim@umyu.edu.ng

dramatically. Many IoT devices have weak security configurations, lack regular updates, and often use default passwords, making them easy targets for DDoS attacks. IoT devices are increasingly used in critical infrastructure sectors such as healthcare, transportation, and energy. DDoS attacks on these systems can have severe public safety and security implications.

The Mirai botnet attack in October 2016 is a notable example, utilizing over 100,000 compromised IoT devices, including routers, video recorders, and surveillance cameras. The attack generated network traffic 40 to 50 times higher than normal, disrupting many Internet services and providers for several hours [4]. Botnets such as Hajime and Reaper have specifically targeted IoT devices, with 90% of all IoT attacks in 2020 involving these botnets. In 2022, there were approximately 10 million DDoS attacks globally, with a significant portion involving compromised IoT devices [5].

DDoS attacks aim to prevent services provided by IoT applications by exhausting network resources with unnecessary traffic. When this traffic is generated by numerous geographically distributed zombie devices, the attack is classified as a DDoS. The increasing frequency and impact of DDoS attacks on IoT devices highlight the critical need for enhanced security measures to protect the rapidly expanding IoT infrastructure [2].

DDoS occurs when the host server is overwhelmed by a large volume of unnecessary requests from geographically dispersed zombie devices. One of the most recognized methods for identifying attacks in both the Internet and other networks is the Intrusion Detection System (IDS). IDS is a software or hardware that automates the intrusion detection process, identifying potential intrusions. It assesses the presence of abnormal behaviors in comparison to the system security policy and indications of a system being under attack, capable of safeguarding the system through real-time responses. With the emergence of abnormal behavior detection technology using traditional machine learning models, intrusion detection systems can now analyze and alert against abnormal behaviors exhibiting significant deviations [6].

The progress in sensing technologies has enabled the establishment of IoT networks. Nevertheless, IoT devices encounter various constraints, such as limitations in energy sources and capabilities. Additionally, conventional cryptography and standard IDS techniques prove inadequate for such networks. Furthermore, as connectivity to the Internet increases, hacking techniques become more robust and easily accessible.

DoS/DDoS attacks are recognized as the common threats that significantly affect the security of IoT (Internet of Things) devices. The main goal of such attacks is to incapacitate targeted systems, making them unavailable to authorized users by deploying harmful malware. DoS seeks to disrupt services provided by IoT applications by overwhelming network resources with unnecessary traffic. On the other hand, DDoS occurs when the host server is overwhelmed with an extensive volume of unwarranted requests from geographically scattered zombie devices.

Consequently, the challenge lies in implementing an efficient monitoring process for intrusion detection. This has spurred numerous research proposals aimed at improving the performance of IoT intrusion detection. To counteract such threats, Intrusion Detection Systems (IDS) play a crucial role. IDS is a monitoring system designed to identify suspicious activities and generate alerts upon detection. These activities, referred to as intrusions, intend to gain unauthorized access to a computer system. IDS can be categorized into Network-based IDS (NIDS), which connects to one or more network segments, scrutinizing network traffic for malicious activities, and Host-based IDS (HIDS), which is linked to a specific computer device, monitoring malicious activities occurring within the system. Regrettably, the current methods suffer. from the following issues:

- Real-time detection rate of attacks,
- Identify new forms of attacks, and
- Insufficient classification rate of attacks.

Hence, the challenge at hand is to present an effective Intrusion Detection System (IDS) solution that addresses the mentioned issues, with a particular emphasis on real-time detection of attacks.

This work aims to design a novel approach for addressing IoT networks vulnerabilities in detection and classification of DoS/DDoS attacks using Kth Nearest Neighbor (KNN) algorithm and dense neural networks, which will detect DoS/DDoS attacks and classify them. In order to enhance the effectiveness of the proposed system, the dataset undergoes a division into training and testing subsets prior to the classification process. This classification categorizes information into either the normal class or the anomaly class.

The remainder of this paper is organized as follows: Section 2 presents the related works. Section 3 briefly explains DoS/DDoS attack detection and classification. Section 4 outlines the design principles considered for the implemented model. Section 5 describes the proposed methodology. Section 6 present results and discussion. Section 7 concludes the paper.

2.0 RELATED WORKS

Due to the emergence of increasingly sophisticated botnets that exploit vulnerabilities in IoT device security, there has been a notable surge in the focus on ensuring security measures for IoT devices in recent times. The study conducted by

[7] proposed employing a deep learning strategy utilizing Convolutional Neural Networks (CNN) to efficiently detect intricate Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks by converting the network traffic dataset into an image format. The methodology involved the transformation of the non-image network traffic dataset into a three-channel image representation. Following this, the CNN model, specifically ResNet, underwent training on the converted dataset, and its effectiveness in identifying recent DoS and DDoS attacks was evaluated. The suggested approach exhibited a high level of accuracy in detecting both DoS and DDoS attacks, demonstrating improved precision in identifying 11 specific types of such attacks. However, it is important to note that these models may not perform optimally when trained on a non-image dataset, as their design is specifically crafted to recognize patterns within images. Moreover, [8] proposed an Intrusion Detection System (IDS) that operates in real-time and adopts an anomaly-based preventive approach for intrusion detection and localization. This approach is designed to be applicable to a broader range of attacks, including Stealthy Distributed Denial of Service (DDoS) attacks. The IDS actively monitors data traffic from connected devices, triggering alarms when sufficient statistical evidence indicates potential threats and blocking them when necessary. The evaluation of the proposed IDS involved the use of a deep autoencoder-based algorithm, which successfully detected all attacks, achieving a 100% true positive rate in terms of attacks, thanks to its sequential nature. The proposed ODIT-based method demonstrated even more accurate and quicker detection compared to the autoencoder-based method. However, a key assumption is that the nominal behavior of devices remains constant over time. In a real system implementation, the IDS would need periodic updates, even though training is required only once.

Also, [9] introduced an innovative method for detecting intrusions in IoT networks by employing deep learning principles. The approach utilized a feed-forward neural network (FNN) model capable of binary and multi-class classification, effectively addressing various attacks like denial of service, distributed denial of service, reconnaissance, and information theft directed at IoT devices. The model relied on generic features derived from individual packet field information to accurately distinguish between normal and malicious traffic, resulting in minimal false positives (FP) and false negatives (FN) predictions. Despite achieving positive outcomes, the study faced certain challenges. In binary classification, the classifier encountered difficulty in discerning embedded packets within malicious traffic, particularly in instances of DDoS over UDP and service scan attacks where a UDP packet was present within the ICMP payload. Additionally, the classifier demonstrated relatively lower precision for data exfiltration and key logging attacks. In multi-class classification, confusion arose in specific attack categories such as reconnaissance and information theft. Despite these challenges, the evaluation of the proposed FNN model revealed an overall commendable classification accuracy.
Furthermore, [10] presented a detection framework specifically crafted to recognize Denial of Service (DoS) attacks at the application layer, particularly those targeting the MQTT protocol. The framework underwent testing in scenarios involving both legitimate activities and protocol-compliant DoS attacks. The primary objective was to protect MQTT message brokers from such attacks, and the proposed framework employed machine learning for detection purposes. Through experimentation, the study illustrated the impact of these attacks on various MQTT brokers and evaluated the effectiveness of the framework in identifying malicious activities. The results indicated that attackers could strain server resources, even in cases where legitimate access to MQTT brokers was denied and resources were limited. The MQTT features identified demonstrated a high level of accuracy in detecting attacks. It is important to note, however, that the framework was trained offline using a generated dataset.

In addition, [11] proposed deep neural network architecture, consisting of seven hidden layers, and is based on feed-forward back-propagation that models multiple application layer DDoS attacks. They proposed an approach to protect Web-based services DDoS attacks by routing traffic through the proposed system and detecting malicious behavior. The malicious behavior of the packets was detected by using pre-learned patterns within the application. It also detects malicious behavior from packets, if an entirely new malicious pattern is being used. In the proposed system, those new patterns would serve as a secondary data set to train the neural network and it automatically tune the hidden layers of ANN to iteratively detect macro patterns in network flows.

Table 1. Comparison of Related Works

Authors	Year	Machine Learning Techniques	Application Domain
[7]	2020	DL	IoT Networks
[8]	2020	ANN	IoT Networks
[9]	2019	FNN	IoT Networks
[11]	2019	ANN	Network Security

3.0 DOS/DDOS ATTACK DETECTION

DDoS (Distributed Denial of Service) attacks are particularly relevant to IoT (Internet of Things) due to several factors. The large number of devices in IoT networks makes them susceptible to being exploited for large-scale DDoS attacks. Many IoT devices lack robust security, making them easy targets for attackers. The diverse and interconnected nature of IoT devices creates multiple vulnerabilities. Additionally, IoT devices often perform critical functions, so DDoS attacks can disrupt essential services. Traditional security solutions may not be effective, requiring advanced real-time detection and traffic analysis to monitor and protect IoT networks. Overall, the distributed, interconnected, and often insecure nature of IoT devices makes them particularly vulnerable to DDoS attacks, necessitating robust detection and mitigation strategies.

Distributed Denial of Service (DDoS) attacks in IoT involves monitoring network traffic for abnormal patterns or sudden spikes in data requests. In the proposed real-time detection, the system analyzes the behavior of connected devices, looking for unusual activity that may indicate a coordinated attack. This can include rapid and excessive data requests, unusual traffic patterns, or an overwhelming number of connection attempts. Employing anomaly detection and traffic analysis mechanisms enhances the ability to identify and mitigate potential DDoS threats in IoT domains.

3.1 Classification of Dos/Ddos Attacks

This project primarily focuses on classification rather than detection, emphasizing the development of a learning model and the identification of relevant features. These components are crucial as they are intended for subsequent use in the detection phase of an Intrusion Detection System (IDS). The classification model is specifically trained to differentiate various types of network traffic patterns. During detection, the trained model and identified features will be integrated into a dedicated detection engine within the IDS framework. This phase will utilize the model to analyze incoming data in real-time, effectively pinpointing potential threats based on classified patterns and features.

Classifying DDoS (Distributed Denial of Service) attacks involves analyzing network traffic patterns for anomalies. In our proposed hybrid model, the kth nearest neighbor (KNN) and dense neural network are trained on normal behavior to identify deviations, utilizing features like traffic volume, packet characteristics, and protocol adherence. Continuous monitoring allows adaptive threat detection. The goal is rapid identification for effective mitigation, minimizing false positives and negatives.

Generally, DDoS attacks aim to disrupt the normal functioning of a target's online services by overwhelming its resources. DDoS attacks are classified into three main types:

- Volumetric Attacks: These overwhelm a target by consuming its network bandwidth.
- Protocol Attacks: Exploit vulnerabilities in network protocols to disrupt services.
- Application Layer Attacks: Target web applications by overwhelming them with a high number of requests.

4.0 DESIGN PRINCIPLES

In this section, we delve into the technical details of our proposed hybrid approach aimed at enhancing the accuracy of real-time intrusion detection and classification. We focus on the efficient utilization of the MQTT-IoT-IDS2020 dataset to achieve superior performance in this context.

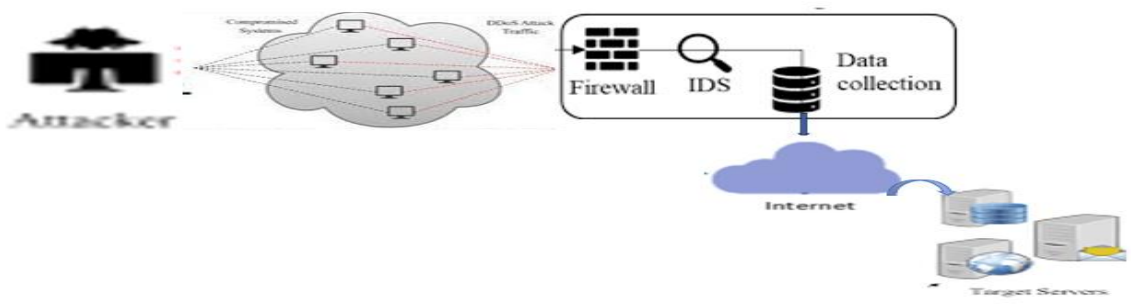

Figure 1. Diagram of the Proposed Intrusion Detection System (IDS)

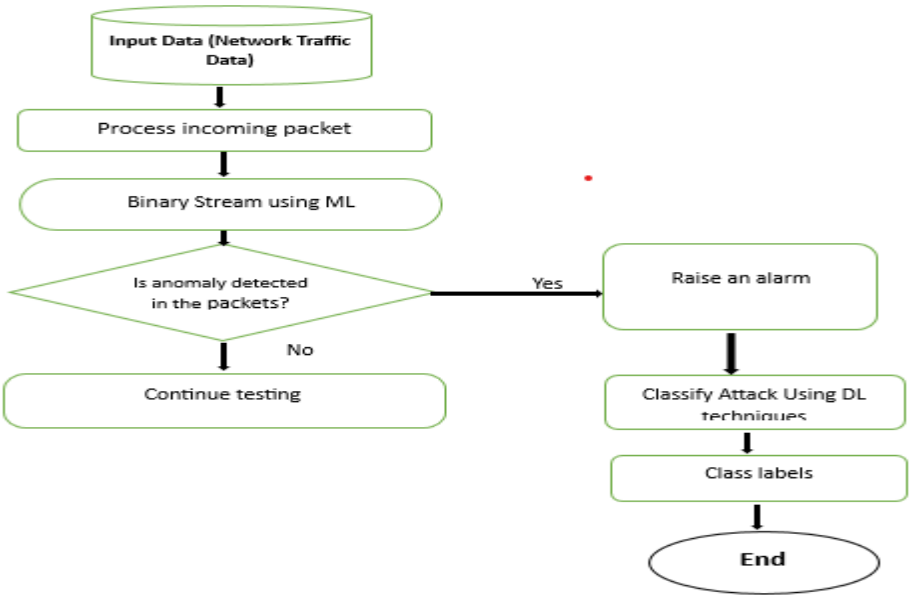

Figure 2. Flowchart of the Proposed Intrusion Detection and Classification Model

4.1 Proposed Real Time Attack Detection and Classification Algorithm

Real-Time Attack Detection and Offline Synchronization Algorithm
Input: a dataset X = [0...n-1] of packets
Output: total categories of attacks detected
Initialize: s = 0, t = 0
isOnline = True
offlineBuffer = []
def attack_detection_online():
for n = 1 to N do
  Partition training set into Dn M1 and DnM2
  Determine Ln(α)
While Mt < hd do
  t = t + 1
  Get new data { Dnt } and compute{ Dnt }
  Mnt = max { Mnt + Dnt , 0 }
  Mt = ∑Nn=1 Mnt
  if Mt >= hd then
    DeclareAttack(T = t)
  end if
end while
def store_offline_data(data):
  offlineBuffer.append(data)
def recover_from_offline():
  global isOnline
  isOnline = True
  for data in offlineBuffer:
    attack_detection_online(data)
  offlineBuffer = []
while True:
  if isOnline:
      attack_detection_online()
  else:
      incoming_data = receive_data()
      store_offline_data(incoming_data)
  if check_online_status():
      recover_from_offline()
for l ∈ [1, L] do:
  Initialize: Wl = 0, bl = 0
  Encoding layer:

Calculate encoding or hidden representation using equation $hn = f\theta(xn) = \sigma(Wxn + b)$
$hl = S\ (Wlxl1 + bl)$
Decoding layer:
while not loss == stopping criteria do:
Compute yl using equation $yl = g\theta(hn) = \sigma(Whn + b)$
Compute the loss function: binary cross-entropy
Update layer parameters $\theta = \{W, b\}$
end while
end for
Classifier: Dense neural network, Soft-max activation at the output layer.

5.0 PROPOSED METHODOLOGY

The intrusion and classification model we proposed was implemented and validated using Python, along with Scikit-learn libraries, within the Jupyter Notebook environment. All evaluations were conducted on a Windows machine equipped with an Intel(R) Core(TM) i5-5300U CPU @ 2.30GHz, with a processing speed of 2.30 GHz.

5.1 Data Acquisition

The initial phase of the proposed methodology involves data acquisition, aiming to gather both regular and attack-related network traffic. Generating a substantial amount of normal and attack traffic in real-time necessitates significant network resources and diverse captures of network activity, making it a demanding task. Setting up a large-scale network also consumes considerable time and financial resources. However, an alternative to going through this exhaustive process is to make use of publicly accessible network traffic datasets. To ensure the dataset's high quality, our analysis focused on specific criteria:

- The dataset should exhibit network traffic in real-time.
- It should be comprehensive and flexible.
- It must contain the latest occurrences of (DoS) and (DDoS) attacks.
- It should cover a range of attack methods.

Based on these criteria, for this specific study, we chose the MQTT-IoT-IDS2020 dataset. This dataset is distinguished by its larger sample size in comparison to other network traffic datasets.

5.2 Pre-processing of the Dataset

This section discusses the techniques applied to ready the dataset for machine learning tasks, involving actions like data cleansing, normalization, and addressing class imbalances. Preparing data is pivotal to ensure machine learning models are prepared for use. Initially, the process involves merging separate files into a cohesive flow network at the Pandas script level. Pandas, a Python library aimed at dataset analysis and manipulation, is utilized for this task. Importing the data file into a Pandas data frame generates a CSV file that encompasses both binary and multi-class label attributes.

5.3 Feature Selection

Initially, we gather traffic packets from the MQTT IoT dataset using the pandas library. Subsequently, we extract relevant fields from individual packets, where each extracted field represents a feature. Rather than computing features based on aggregated packets, we utilize the field information of individual packets as features. This approach aims to capture generic traffic features instead of generating features tailored to specific attack behaviors. Specifically, we mainly focus on header fields in the IP packet, which include frame and TCP/UDP related information.

To counter the class imbalance, Synthetic Minority Oversampling Technique (SMOTE) is used. This method tackles the scarcity of certain class instances by generating synthetic data points. It does so by creating new instances within the minority class, interpolating between existing ones, as described by [12]. To ensure fairness and prevent bias, the dataset is shuffled before applying SMOTE. Evaluating the model's effectiveness includes partitioning the dataset into training and testing subsets, maintaining a 70:30 ratios.

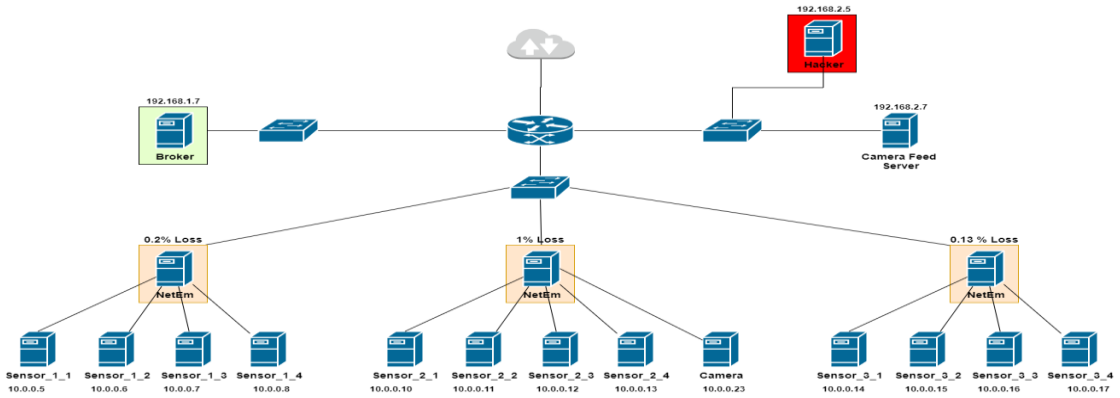

Figure 3. MQTT-IoT-IDS2020 Network Architecture [13]

6.0 RESULTS AND DISCUSSION

This section describes the performance measures used which include accuracy, multi-class roc curve, speed of detection.

6.1 Performance Measures

Accuracy assesses the reliability of the Intrusion Detection System (IDS) in distinguishing between normal and abnormal traffic behavior. It is calculated as the percentage of all instances correctly predicted, using the following formula:

Accuracy=(TP+TN)/(TP+TN+FP+FN)

Where TP is true positive, TN is true negative, FP is false positive, and FN is false negative.

6.2 Confusion Matrix for Multi-Class Classification

Figure 4 displays the confusion matrix for the multi-class classification. In multi-class classification, the context of packets typically involves categorizing network packets into more than two classes or categories. Each packet contains information transmitted over a network, and classifying them can help in various network-related tasks such as intrusion detection, and traffic analysis. Figure 4 displays the confusion matrix of the model obtained from 114893 packets in the dataset, there are a total of 5702 attack flows that are incorrectly reported as legitimate flows and 489 instances of legitimate flows that have been falsely announced as a malicious attack. However, 89315 legitimate packets are correctly classified.

Actual Class \ Predicted Class						
Bruteforce	**2702**	894	00	145	489	84
DOS	452	**35751**	00	2444	156	117
Flood	00	21	**75**	66	02	01
Legitimate	00	1300	00	**48234**	12	221
Malformed	888	736	00	243	**1284**	79
Slowrite	147	751	00	447	68	**1379**

Figure 4. Confusion Matrix of Classified Data

6.3 Multi-class ROC graph

ROC: ROC, or Receiver Operating Characteristics, is a curve that plots the true positive rate against the false positive rate of a model. The area under the curve (AUC) serves as a metric for assessing the performance of a classification model. AUC offers a comprehensive measure of performance across all possible classification thresholds. A threshold is a point along the graph line. ROC curves enable the comparison of multiple models. Models with curves closer to the top-left corner (having higher true positive rates and lower false positive rates) are generally considered better. In figure 5 we can see that the proposed, did better in correctly classifying the six classes of attacks by covering more area therefore having better AUC since the more AUC, the better performance.

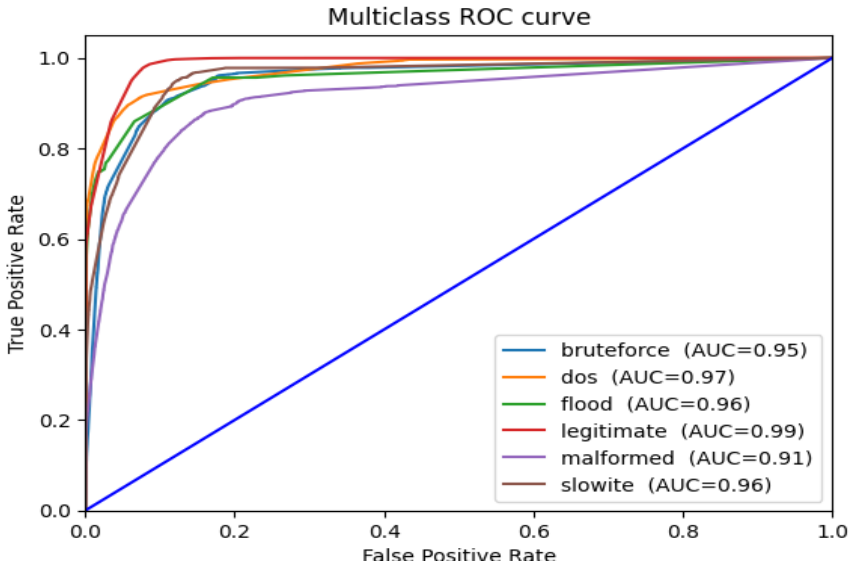

Figure 5. Multiclass Roc Curve

6.4 Speed of Detection

In multiclass attack detection, the speed of detection refers to the efficiency with which a system can promptly identify and categorize various types of attacks. In real-time applications, a swift time-to-detection is crucial for timely responses and minimizing the impact of security incidents. However, achieving a balance between speed and accuracy is vital to avoid false positives, ensuring that normal activities are not misinterpreted as attacks. Multiclass attack detection systems are tasked with not only detecting attacks but also classifying them into distinct categories.

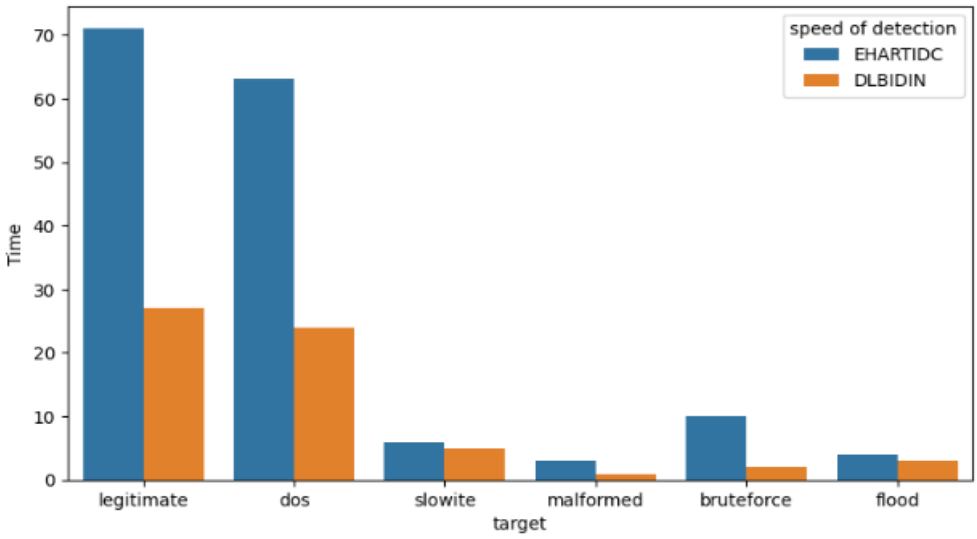

Figure 6. Speed of Detection

In figure 6 we can see that the proposed enhance algorithm for real time intrusion detection and classification (EHARTIDC), did better than its counterpart, as proposed by [14] Deep Learning-based Intrusion Detection for IoT Networks (DLBIDIN) algorithm for both binary and multiclass classification which has better performance.

6.5 Accuracy

Similar to several other studies conducted on this dataset using machine learning techniques, this study utilizes multiclass classification techniques and compared the proposed Enhanced Hybrid Algorithm for Real Time Intrusion Detection and Classification (EHARTIDC) with that of [15] which is the Efficient Deep Learning Model For Intrusion Classification and Prediction (EDLMICP). Unlike binary classification, which predicts two outcomes, multiclass classification is employed here to categorize flows into multiple classes. Specifically, it aims to predict the flow's classification among various classes such as 'Attack,' 'Benign,' and potentially other distinct types. The model is trained using a multiclass setup with 10 epochs, determined to provide an optimal balance between training time and accuracy.

Looking at figure 7, we can conclude that the algorithm proposed in this study, that is EHARTIDC, performs better than the one in the work of [15], that is EDLMICP.

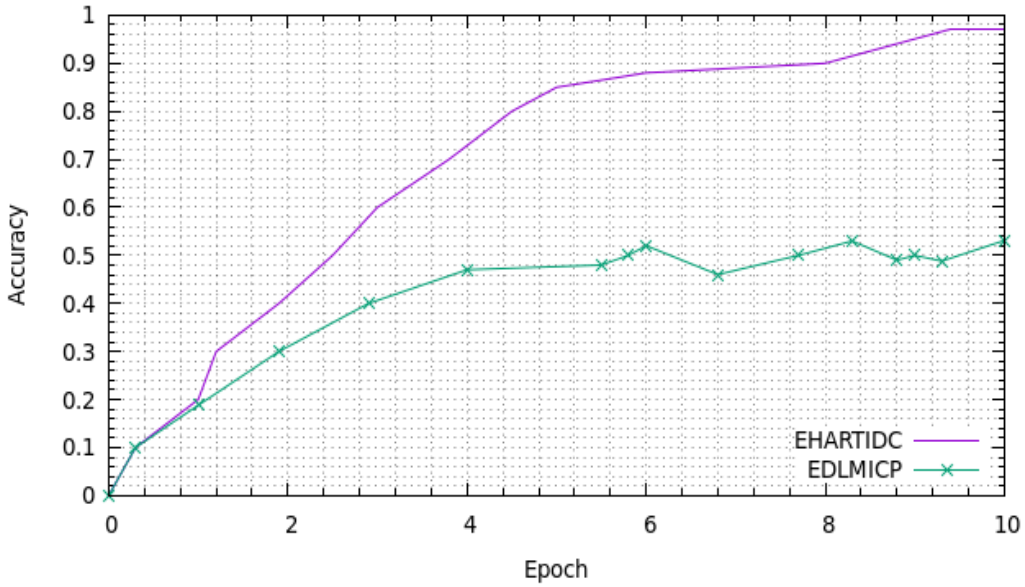

Figure 7. Accuracy of the model

The overall accuracy of the proposed EHARTIDC model, which employs Kth Nearest Model and Dense Neural Network, reaching up to 97% which is higher than similar experiments conducted by **[15]**. This reinforces the accuracy of the results, indicating minimal occurrences of false positives and false negatives. This validation supports the authenticity of the detection and classification of attacks through this method.

7.0 CONCLUSIONS

In this study, the hybrid approach for intrusion detection and classification in IoT environment was explored. The research builds on the work of [15] and it was conducted by analyzing network flow data. The main aim of this research was to analyze and classify intrusions into Internet of Things networks offline and in real time. Therefore, we adopted the simulated MQTT-IoT-IDS2020 dataset due to its recency and that fact that it reflects ideal IoT settings provides legitimate traffic. After labeling the dataset, K-nearest neighbor algorithm was used to train the model on the dataset to achieve an effective online model. After evaluating the classifiers on the entire dataset, we tested it with 30% of the dataset while 70% was used for training. Then, the performance was evaluated using confusion matrix and learning curves.

The methodologies employed in this research demonstrated to be effective in addressing the inherent class imbalance within the MQTT-IoT-IDS2020 dataset. Utilizing SMOTE for synthetic sample generation and adjusting class weights played a crucial role in achieving this balance, leading to an overall enhancement in model performance. The findings of the study underscored the importance of large hyper parameter tuning to optimize model effectiveness. Consequently, within an extensive hyper parameter space, the tuning of hyper parameters proved to be a highly valuable approach.

While the results of this research were predominantly positive, they also highlighted aspects that could be enhanced through further refinement. Subsequent efforts should explore advanced oversampling techniques or alternative strategies for addressing class imbalance. Additionally, considering the model's effectiveness in predicting specific types of attacks, it is advisable to conduct additional validations on diverse datasets to ensure the models exhibit robust generalization across various scenarios and attack types.

ACKNOWLEDGEMENTS

This study was not supported by any grants from funding bodies in the public, private, or not-for-profit sectors.

AUTHORS CONTRIBUTION

Abubakar Aminu Muazu (Formal analysis; Visualisation; Supervision)

Aisha Ibrahim Gide (Conceptualisation; Methodology; Data curation; Writing - original draft; Resources)

CONFLICT OF INTEREST

The authors declare no conflicts of interest

REFERENCES

[1] M. Z. e. al., "Protocol-Based Deep Intrusion Detection for DoS and DDoS Attacks Using UNSW-NB15 and Bot-IoT Data-Sets, IEEE Access, vol. 10, pp. 2269-2283, 2022, doi: 10.1109/ACCESS.2021.3137201, 2022.

[2] R. K. a. D. Eleyan, "Survey of DoS/DDoS attacks in IoT," *Sustainable Engineering and Innovation ISSN 2712-0562*, p. 7, 2021.

[3] Barati, "Distributed Denial of Service Detection Using Hybrid Machine Learning Technique," *International Symposium on Biometrics and Security Technologies (ISBAST)*, p. 6, 2014.

[4] L. Huraj, "IoT measuring of UDP-based Distributed Reflective DoS Attack," *SISY 2018 • IEEE 16th International Symposium on Intelligent Systems and Informatics • September 13-15, 2018, Subotica, Serbia*, p. 6, 2018.

[5] B. Stackpole, [Symantec](https://www.symantec.com/blogs/feature-stories/iot-attacks-rise), 2020.

[6] Y. Wu, "Network Attacks Detection Methods Based on Deep Learning Techniques: A Survey," *Security and Communication Networks Volume 2020, Article ID 8872923,* , p. 17, 2020.

[7] Hussain, "IoT DoS and DDoS Attack Detection using ResNet," *2020 IEEE 23rd International Multitopic Conference (INMIC), Bahawalpur, Pakistan, 2020, pp. 1-6,* , p. 7, 2020.

[8] Y. Y. a. S. U. Keval Doshi, "Timely Detection and Mitigation of Stealthy DDoS Attacks via IoT Networks," *https://doi.org/10.48550/arXiv.2006.08064*, p. 13, 2020.

[9] Ge, "Deep Learning-based Intrusion Detection for IoT Networks," *2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC),* p. 10, 2019.

[10] Z. B. ,. A. I. &. C. V. Naeem Firdous Syed, "Denial of service attack detection through machine learning for the IoT," *Journal of Information and Telecommunication, DOI: 10.1080/24751839.2020.1767484*, p. 23, 2020.

[11] Asad, "DeepDetect: Detection of Distributed Denial of Service Attacks Using Deep Learning," *The British Computer Society 2019. All rights reserved.*, p. 12, 2019.

[12] Munshi, Novel ensemble learning approach with SVM-imputed ADASYN features for enhanced cervical cancer prediction07, https://doi.org/10.1371/journal.pone.0296107, 2022.

[13] R. A. B. A. a. X. Hanan Hindy, "MQTT-IOT-IDS2020: MQTT INTERNET OF THINGS INTRUSION DETECTION DATASET," 2020.

[14] G. X. F. &. Z. B. Mengmeng, "Deep Learning-based Intrusion Detection for IoT Networks," *2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC),* p. 10, 2019.

[15] Rezvy, "Intrusion Detection and Classification with Autoencoded Deep Neural Network," *Springer Nature Switzerland AG J.-L. Lanet and C. Toma (Eds.): SecITC LNCS 11359, pp. 142–156,*, p. 15, 2019.

[16] S. F. C. H. B. A. H. R. R. Mohammad, "Classification and Detection ofMalicious Attacks in Industrial IoT Devices via Machine Learning," *K.-Y. Kim et al. (Eds.): FAIM 2022, LNME, pp. 99–106, 2023.https://doi.org/10.1007/978-3-031-18326-3_10*, p. 10, 2023.

[17] Doshi, "Timely Detection and Mitigation of Stealthy DDoS Attacks via IoT Networks," *https://doi.org/10.48550/arXiv.2006.08064*, p. 13, 2020.

[18] Rezvy., "An efficient deep learning model for intrusion classification and prediction in 5G and IoT networks," *978-1-7281-1151-3/19/$31.00 ©2019 IEEE*, p. 6, 2019.

[19] F. S. Z. B. ,. A. I. &. C. V. Naeem, "Denial of service attack detection through machine learning for the IoT," *Journal of Information and Telecommunication, DOI: 10.1080/24751839.2020.1767484*, p. 23, 2020.