مجلة المجد العلمية المتطورة العدد (5) المجلد (5) تموز 2025

تعزيز هجومDDoS

Enhancing DDoS attack

مجد ثائر حامد رشيدات، تخصص/ أمن سيبرانني، جامعة اربد الأهلية، اربد، فلسطين

تاريخ الاستلام: ٢٠٢٥/٦/٩ تاريخ القبول: ٢٠٢٥ /٦/١٩ تاريخ النشر: ٢٠٢٥/٧/١٥

هذا العمل مرخصة بموجب Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International.
 الحقوق الفكرية (c) 2025 مجلة المجد العلمية المتطورة

Enhancing DDoS attack

الملخص:

تُشكل هجمات رفض الخدمة الموزعة (DDoS) تحديًا كبيرًا لشبكات الحاسوب والأنظمة المختلفة، لا سيما في العديد من المجالات، بما في ذلك أمن إنترنت الأشياء والحوسبة السحابية. تعتمد سلامة وأداء الأعمال في هذه المجالات، بما في ذلك إنترنت الأشياء (IoT)، بشكل كبير على قدرتها وإمكانياتها على تحديد ومنع هجمات الخدمة الموزعة (DDoS) داخل شبكات إنترنت الأشياء. ومن بين الطرق أيضًا الكشف المبكر عن هذه الهجمات داخل بيئة الحوسبة السحابية. يوفر هذا التحليل العلمي عدة طرق للكشف المبكر عن هجمات رفض الخدمة الموزعة والاستجابة لها. توفر النتائج المستمدة من هذا البحث العلمي معرفة مهمة لتحسين آليات السلامة لأجهزة إنترنت الأشياء وداخل بيئات عمل الحوسبة السحابية، في سياق هجمات رفض الخدمة الموزعة (DDoS). تؤكد المنهجيات المدعومة على ضرورة وفعالية استراتيجيات المعالجة المسبقة المناسبة لصياغة أنظمة آلية قوية داخل البنى التحتية لإنترنت الأشياء والحوسبة السحابية.

الكلمات المفتاحية: تعزيز هجوم رفض الخدمة الموزع.

Abstract:

Distributed Denial of Service (DDoS) attacks pose a major challenge to computer networks and various systems, especially in several areas including Internet of Things security and cloud computing. The safety and performance of business in these areas, including the Internet of Things (IoT), strongly depends on its ability and capabilities to identify and prevent distributed service (DDoS) attacks within IoT networks. One of the methods is also the early detection of these attacks within a cloud computing environment. This scientific analysis provides several methods for early detection and response to DDoS attacks. The results derived from this scientific research provide important knowledge to improve safety mechanisms for Internet of Things devices and within cloud computing work environments, In the context of distributed denial of service (DDoS) attacks. The supported methodologies emphasize the necessity and effectiveness of appropriate preprocessing strategies to formulate robust automated systems within IoT and cloud computing infrastructures.

Keywords: Enhancing DDoS attack.

.

Introduction

In recent technological developments over the past years, technology has witnessed a major renaissance in many aspects. One of the most important of these modern technological developments is the concept of cloud computing and the Internet of Things [1,5]. By the concept of cloud computing, we mean the possibility of obtaining services from the Internet, and cloud computing (CC) provides a wide and exceptional set of tools. Technical resources and methodologies that provide services through an Internet connection, which also enable users to take advantage of the software and hardware systems located within data centers [1]. By the concept of the Internet of Things (IoT), that it is many devices linked together in one network that work together in an interconnected manner [5]. Cloud computing constitutes a qualitative shift in the technology community that works to connect things on the Internet with the aim of creating an integrated environment connected to the Internet to enable the world to communicate. Better access to services as well.

It is known that any system or services provided over the Internet are vulnerable to distributed denial of service (DDoS) attacks are widespread and cause serious problems and damage to systems on the Internet. From this standpoint, there is an increasing need to ensure the safety and security of services provided on the Internet in real time [4]. In the Internet of Things and cloud computing systems, it must be ensured that the network devices are capable of confronting this type of attacks. And work to prevent and reduce its occurrence to avoid damage to systems and services uploaded to the Internet.

Much ongoing research work has been obtained that deals with the concept of distributed service attacks (DDoS) to identify and respond to these attacks [1, 2, 3, 4, 5, 6] Some of these works are specialized in a specific field and some are specialized in several fields. Some works [5] used the NSL-KDD dataset as input, and applied measurement and cryptographic techniques to counter the attacks. Some works [1] applied an advanced framework for real-time detection and prevention of DDoS attacks in the cloud using deep learning techniques. [6] framework has been implemented for real-time DDoS attack detection and mitigation in SDN-enabled smart home networks. Some works [3] developed the M-RL system, to detect UDP DDoS attacks. [2] implements an improved DDoS attack detection method using hybrid feature selection technique in combination with ensemble-based classifiers. This work aims to clarify some methods to confront DDoS attacks in different systems, and among these systems.

In the Internet of Things (IoT) system, a methodology based on Principal Component Analysis (PCA) and one without Principal Component Analysis (PCA) has been developed to compare them and implement robust cryptographic systems. This methodology has helped in enhancing IoT security and has responded with high accuracy in detecting DDoS attacks on IoT devices [5].

Cloud Computing System (CC) The (DeepDefend) framework is used to detect DDoS attacks in cloud computing systems, and attacks are detected in real time to address them in the cloud computing environment. This methodology relies on the use of genetic algorithms with the (DeepDefend) framework that work together to enhance the effectiveness of the (AutoCNN-DT) model so that the model can accurately distinguish between normal movement and attack movement to confront it. This methodology has been applied to CNN-LSTM

https://scopmajd.com/ « ISI: (0.841) « ISSN (Online): 3005-2033

networks, and results have shown improved and accurate detection and response against DDoS attack threats to improve and protect cloud computing [1].

2. Related works

With the modern technological development in various systems, these systems face the greatest challenges represented by various attacks that work to weaken or destroy them. The most dangerous of these attacks are those that destroy systems connected to the Internet. DDoS attacks have been a major fear for most Internet of Things (IoT) and Cloud Computing (CC) systems, so many researchers have provided many researches, solutions, and methods to counter, detect, and prevent these attacks. The researchers in [3] used the M-RL system, which consists of an IDS device compatible with easy movement capabilities. This system takes care of the UDP flow and takes into account the RL method and spoofing threats using the RSS method. The researchers developed a method capable of evaluating and comparing the (M-RL) system, using RL and RSS algorithms to detect malicious attacks. Then design in [6] a real framework for detecting DDoS attacks. Networks that support SDN were used, such as modern home networks, and the researchers worked on using models such as traditional ML and SVM. The framework works to detect and protect the SDN controller using SNORT IDS and IoT devices from various DDoS attacks. This is done using machine learning models. Researchers [4] developed an improved system to detect and respond to dual attacks, both malicious (DDoS) and non-malicious, using HRDPA data preprocessing technology. They worked to use the best models. Tuned parameters were optimized through logistic regression, decision tree, and random forest algorithms to obtain the best parameters. Finally, a new Deep Grid network was developed that uses machine learning classifiers LC, RF, DT, and NB. This proposed method proved that the proposed models are the most effective in detecting harmful and non-harmful dual DDoS attacks. Researchers [2] developed an improved method for detecting DDoS attacks using a hybrid and ensemble-based feature selection method. This ensemble-based approach combines as many models as decision trees to improve classification accuracy, reduce unnecessary equipment, and increase the efficiency of the models used. The method has been proven by researchers. Best results for accurate detection of DDoS attacks.

3. Methodology

In this section we explain DDoS defense methods in IoT and cloud computing systems. We divide it into subsections that explain previous literary works. Since the goal of this work is to target DDoS attacks, we divided the previous work into inputs, methodology, and outputs. We focused on two systems to work on: the Internet of Things system and the cloud computing system [1,5].

3.1. INPUTS

The inputs in this paper consist of a variety of data. This data provides information about network traffic, including source and destination IP addresses, port numbers, transport protocols, timestamps, duration, data size, TCP flags, class labels, attack types, and unique identifiers for attacks. Through this data, a comprehensive analysis can be performed to identify and detect attacks in an accurate manner. Table 1 reviews the methodological inputs

3.2. METHODOLOGY

The methodology proposed in this paper, called Deep Defend, provides a comprehensive approach to detect and prevent DDoS attacks within cloud environments. This methodology consists of seven basic components: traffic collection, clustering, entropy prediction, attack prediction, validator, feature preprocessing, and classification. This process begins with the traffic collection component, the idea of which is to collect data from network front-end devices. This data is then subjected to clustering using a custom time window algorithm. Next, the entropy prediction component uses historical data to predict the entropy of vertex features. The attack prediction component then classifies these windows as “normal” or “anomalous.” When an anomalous window is detected, feature preprocessing components are immediately activated to detect, disrupt, and respond to potential DDoS attacks using flow classification techniques to ensure that the system is working accurately, the Process Verification component checks when data windows are classified as normal. It calculates entropy per minute and this information is fed to the attack predictor, providing the opportunity to correct any prediction errors and enhance accuracy in predicting potential anomalies or attacks on the system. This system continues to operate continuously without interruption, ensuring effective detection and response to DDoS attacks. fig. 1,2 and 3 provide a comprehensive overview of the proposed methodological framework.

Table1 Features description of the dataset.

Feature	Description
Src IP	Source IP address of the traffic origin.
Src Port	Source port number indicating the specific application or service on the source device.
Dest IP	Destination IP address representing the destination of the network traffic.
Dest Port	Destination port number specifying the application or service on the destination device.
Proto	Transport protocol used for transmitting data packets (e.g., ICMP, TCP, UDP).
Date first seen	Timestamp indicating when the flow was first observed by the detection system.
Duration	Duration of a specific flow, representing how long it lasted.
Bytes	Numeric value indicating the number of bytes transmitted during each flow.
Packets	Numeric value indicating the number of packets transmitted during each flow.
Flags	Concatenation of all TCP flags associated with the flow.
Class	Class label assigned to each record, categorizing them as normal, attacker, victim, suspicious, or unknown.
AttackType	Type of attack that occurred within each record (e.g., portScan, DoS attacks).
AttackID	Unique identifier grouping flows belonging to individual attacks.
Description	Additional information about the attack, such as attempted password guesses for SSH brute force attacks.

In the initial phase, the system collects various data from network front-end devices. This collected data includes various parameters related to network traffic and forms the basis for subsequent

During the second phase of the methodology, the system arranges the collected data using a time window algorithm. This method facilitates comprehensive analysis of network traffic patterns over

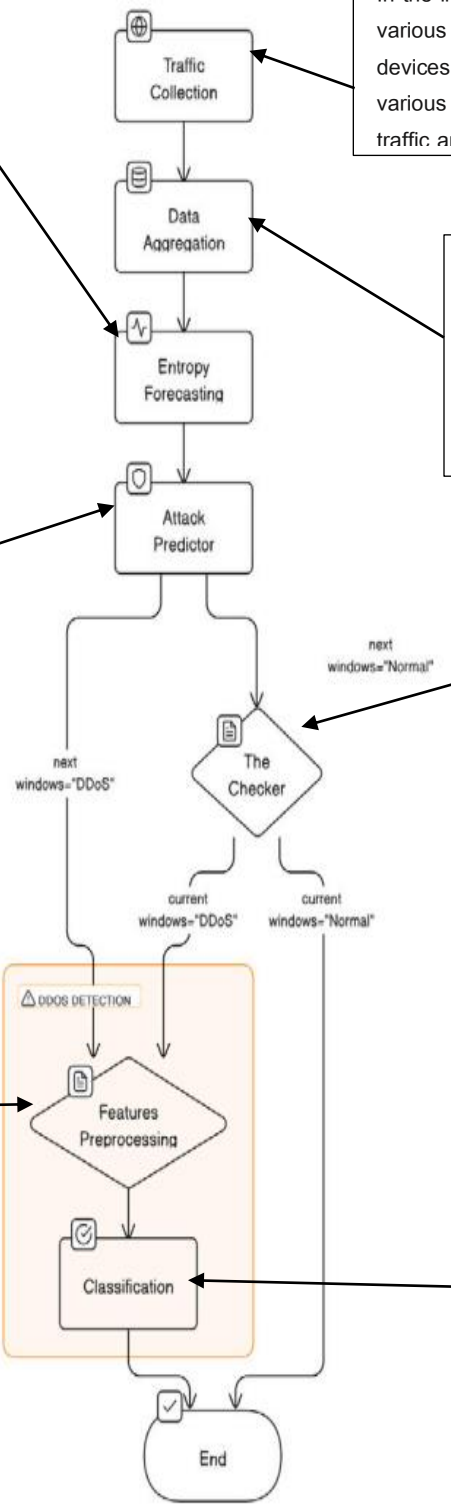
For maximum accuracy, the system continuously monitors the entropy of incoming data flows in real-time.

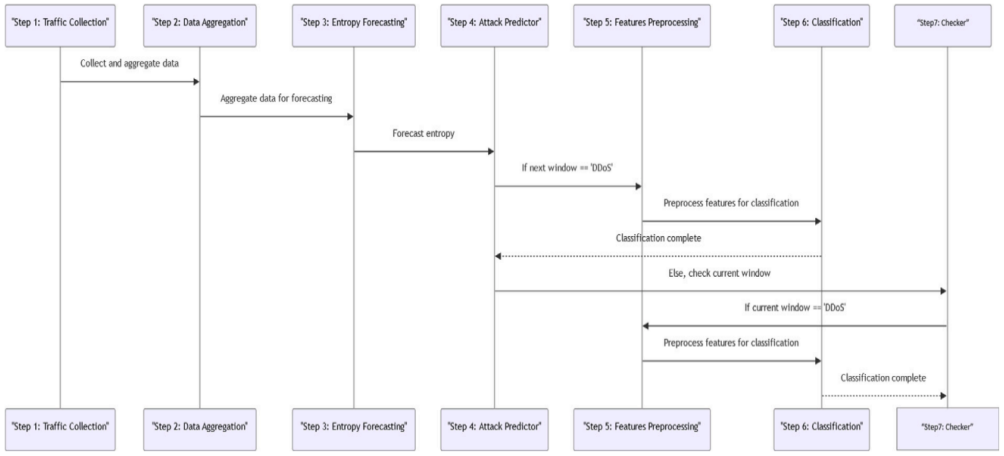
In the final stage, the system uses classification techniques to classify detected DDoS attacks according to their distinctive characteristics.

The collected network traffic data undergoes pre-processing to extract features and detect potential DDoS attack patterns using genetic algorithm. This pre-processing phase increases the system's ability to accurately detect and distinguish

In the fourth stage of the methodology using predicted entropy, the attack prediction component classifies time windows as normal or anomalous. This important process enables the system to distinguish between valid network traffic and

In the third stage, by leveraging historical data, the system uses entropy prediction techniques to predict the entropy of vertex features. This prediction process provides important insights into expected network traffic patterns, enabling the system to





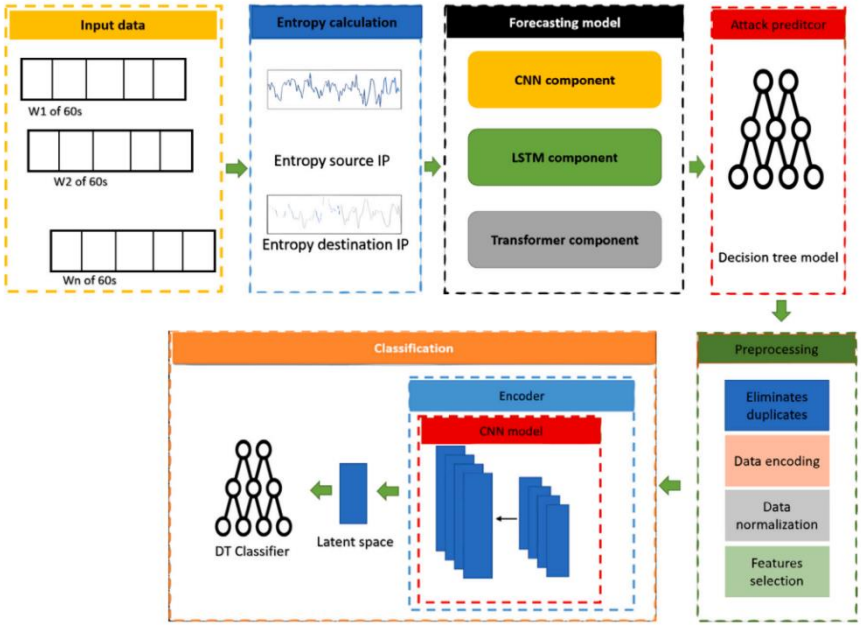


fig.3. The (DeepDefend) framework implements real-time DDoS detection and prevention using a combination of (CNN-LSTM-Transformer) and (AutoCNN-DT) models. The (CNN-LSTM-Transformer) model predicts entropy at 60-second intervals and forwards this data to the attack predictor. The predictor evaluates whether the subsequent time window displays signs of a potential DDoS attack. Here the (AutoCNN-DT) model intervenes to confirm the actual and real existence of the attack. Before the verification phase, a preprocessing phase occurs, and the priority for optimal feature selection is determined by a genetic algorithm. These ideal features are then used by (AutoCNN-DT) to determine whether the current time window represents an attack or normal behavior.

3.3. OUTPUTS

The methodology proposed in the paper introduces (DeepDefend) as an innovative solution for det Fig. 2. The sequence diagram of the proposed framework. attacks within storage cloud environments. It revolves around integrating deep learning and machine learning principles. This approach significantly enhances early detection of DDoS attacks by emphasizing entropy

across diverse systems on the Internet. By doing so it addresses limitations and complexities inherent in cloud environments. Notably this methodology minimizes the utilization of system resources compared to traditional approaches which often impose heavier resource burdens.

3.4. INPUTS

This stage forms is the basis for the methodology described in the paper. The NSL KDD dataset serves as the building block on which machine learning models are built. This dataset includes a wide range of recorded attacks, comprising 125,973 packets and including 22 different types of interactions. (You can access the dataset at https://www.unb.ca/cic/datasets/nsl.html.) Originally designed to detect distributed denial-of-service attacks across devices within the Internet of Things, it provides a rich resource for training and testing the effectiveness of detection algorithms different. Table 4 shows the methodology inputs

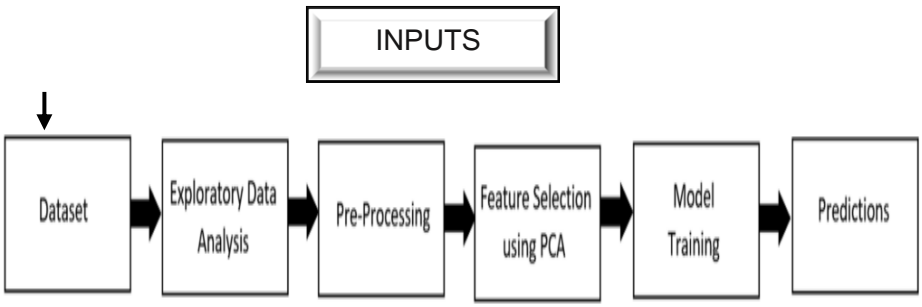


Fig. 4. Proposed Machine Learning

3.5. METHODOLOGY

The methodology development process, shown in Figure 5, includes several basic stages on which the proposed methodology depends. Starting from the first stage, which is the input data set that is processed, it moves to the second stage, during which exploratory data analysis (EDA) is performed to obtain deeper and more accurate insights into the data. To address issues such as missing data, duplication, and normalized features, preprocessing techniques are used. At this stage, Principal Component Analysis (PCA) is used to select features and determine the most relevant characteristics. The refined data set is then put to work training various machine learning algorithms capable of accurately classifying Distributed Denial of Service (DDoS) attacks. Model performance is evaluated using metrics including F1 score, recall, precision, and precision. This comprehensive methodology aims to enhance the DDoS attack detection model on IoT devices by utilizing appropriate dataset, efficient pre-processing, selection of diverse features and classifiers, and rigorous and accurate model evaluation.

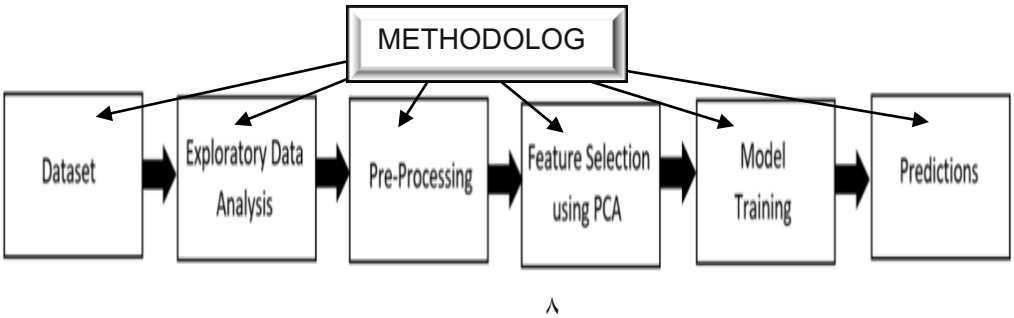


Fig. 5. Proposed Machine Learning

3.6. OUTPUTS

This study focuses on using the NSL-KDD dataset to explore how machine learning algorithms can effectively monitor, detect, and prevent distributed denial of service (DDoS) attacks targeting Internet of Things (IoT) devices. Six different machine learning classifiers were used to measure their effectiveness and accuracy in identifying and detecting such attacks. These classifiers were evaluated with and without prior application of principal components analysis (PCA). Table 1 and Table 2 show performance comparisons of the classifiers. Without using PCA and using PCA, visual representations of Table 2 and Table 3 are shown in Figure 6 and Figure 7 respectively. The results show that the Random Forest classifier consistently outperforms others, exhibiting high accuracy, precision, recall, F1 score, and kappa coefficients in correctly identifying DDoS attacks. While Naïve Bayes showed relatively weaker performance, K-Nearest Neighbor and Decision Tree classifiers showed strong results. It should be noted that the inclusion of PCA generally enhanced the performance of the classifiers, improving the results of precision, recall, F1 score, precision, and kappa coefficient values. The study confirms the effectiveness of machine learning classifiers in detecting DDoS attacks on IoT devices, with the Random Forest classifier combined with PCA emerging as a detection and feature selection method being of particular interest in this context.

2

Table 1
Performance Comparision of ML Classifiers without using PCA.

	Precision	Recall	F1-Score	Accuracy	Kappa
Random Forest	0.9970	0.9987	0.9978	0.9980	0.9245
K-Nearest Neighbour	0.9898	0.9914	0.9906	0.9912	0.9964
Decision Tree	0.9521	0.9669	0.9595	0.9624	0.9824
Support Vector Machines Linear	0.9772	0.8753	0.9234	0.9243	0.7847
Logistic Regression	0.9123	0.8649	0.8880	0.8924	0.8923
Naïve Bayes	0.1903	0.8093	0.3082	0.6007	0.1584

3

Table 2
Performance Comparision of ML Classifiers using PCA.

	Precision	Recall	F1-Score	Accuracy	Kappa
Random Forest	0.9979	0.9994	0.9986	0.9987	0.9473
K-Nearest Neighbour	0.9901	0.9914	0.9908	0.9914	0.9976
Decision Tree	0.9795	0.9648	0.9721	0.9737	0.9827
Support Vector Machines Linear	0.9446	0.9865	0.9651	0.9680	0.8013
Logistic Regression	0.9041	0.8861	0.8951	0.9009	0.9371
Naïve Bayes	0.8011	0.9129	0.8534	0.8714	0.7397

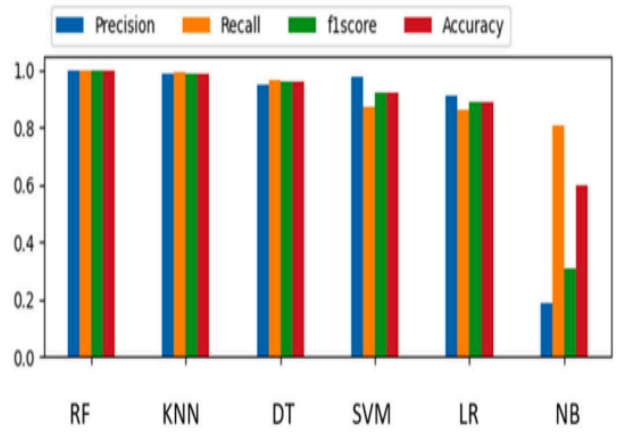


Fig. 6. Classifiers without using

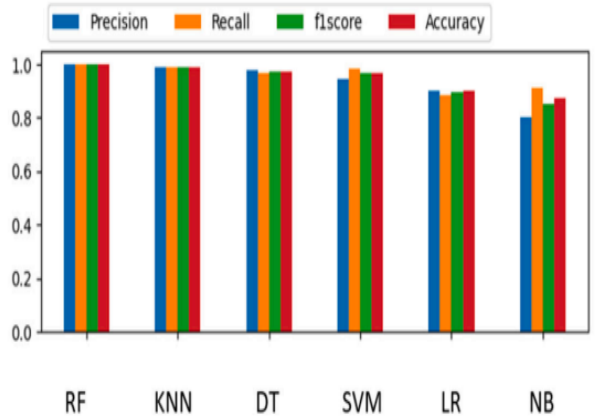


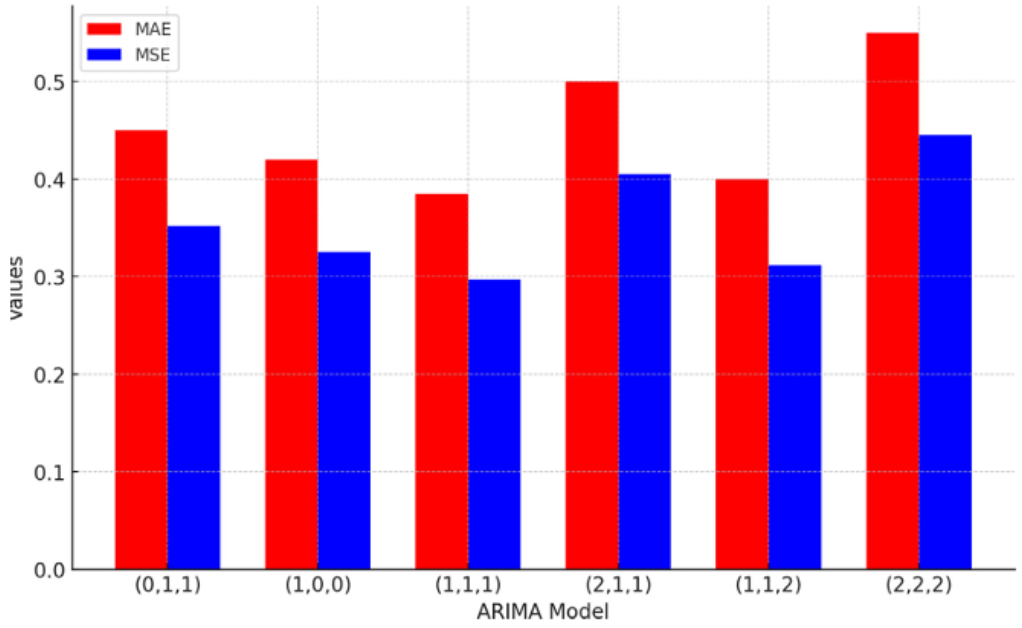
Fig. 7. Classifiers using

4. Results and discussion

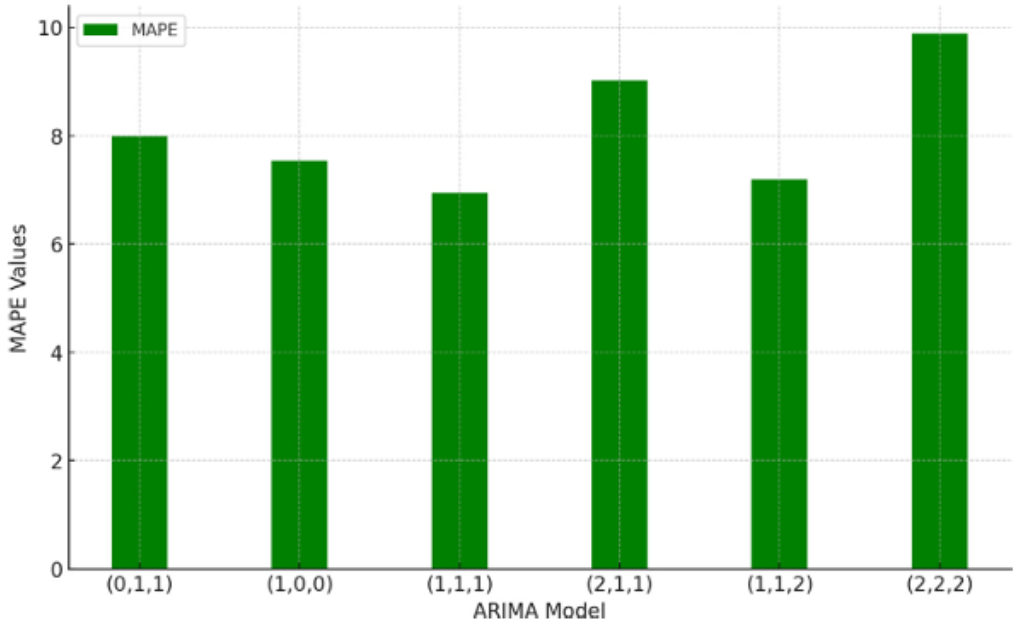
In this section, the results will be presented, and the results reached by the researchers from the works presented in the scientific papers will be discussed [1,5].

Researchers in [1] reached several results, table 4 and Figures 8 and 9 show different results of the ARIMA forecasting performance using metrics such as MSE, MAE and MAPE. An analysis of the performance of the proposed prediction models was conducted. In particular, ARIMA and deep learning architectures. Measures were applied to judge the quality of the proposed models, such as MSE, MAE, and MAPE. The ARIMA (1,1,1) model showed superior accuracy and quality in predicting the entropy of source IP addresses, and this is evident by obtaining the lowest scores for MSE, MAE, and MAPE, and this indicates its high accuracy and effectiveness compared to other models. In addition to that, the ARIMA models were presented (1,0,0) and (1,1,2) perform fairly well. In contrast, the ARIMA (2,1,1) and (2,2,2) models did not provide good results, their accuracy was low. In predicting the entropy of facial IP addresses, it was found that the performance of the ARIMA (2,1,1) model was It provided the best results by obtaining the lowest MSE and MAPE scores, while the ARIMA model (2,2,2) showed the lowest results in terms of accuracy. Relatively speaking, deep learning architectures such as LSTM-Encoder, Transformer, and CNN-LSTM-Transformer obtained the highest accuracy scores, in contrast to models such as ARIMA and other less complex models. The Transformer model was able to achieve good improvement compared to the ARIMA (1,1,1) model in terms of its use on small and medium projects. Moreover, both the Transformer and CNN-LSTM-Transformer models provided 5% lower errors in the results by using MAPE, which indicates its reliability and strong security in identifying data patterns and enhancing attack prediction. Overall, the study demonstrated that advanced deep learning architectures, including LSTM-Encoder, CNN-LSTM-Transformer, and Transformer, are powerful and effective in detecting security threats to cloud computing systems, surpassing traditional models such as ARIMA and less complex deep learning models such as CNN. and LSTM, table 5 summarizes the most important results obtained from the scientific paper.

Table 4



MSE	MAE	MAPE	COMMENTS



ARIMA (1,1,1)	**LOW**	**LOW**	**LOW**	**The best model for detecting source IP changes.**
ARIMA (2,1,1)	**LOW**	**LOW**	**MODERATE**	**Fairly good for predicting the destination IP address.**
LSTM-Encoder	**LOW**	**LOW**	**LOW**	**Outperforms ARIMA, CNN, and LSTM models.**
Transformer	**LOW**	**LOW**	**LOW**	**Significantly better improvement compared to the ARIMA model.**
CNN-LSTM-Transformer	**LOW**	**LOW**	**LOW**	**The best model in all standards.**

The researchers presented several results in [5] that they reached. In the scientific paper, the researchers worked on conducting an experiment on a Dell Inspiron 5567 laptop that runs on Windows 11 Pro. At first, the researchers worked on pre-processing the data using a powerful metric. To do so, they used Principal Component Analysis (PCA), to reduce the size of the features of a random dataset from 42 to 20 dimensions. Work was then done on training, improving, and evaluating several machines learning classifiers, using original and reduced feature sets. Performance metrics were calculated through accuracy, precision, recall, F1 score, and kappa coefficient, and confusion matrices were used to evaluate the performance of the classifiers in detecting DDoS attacks in IoT devices. Figure 10 and 11 shows visual representations in the form of histograms and ROC curves to show the performance for classifiers with and without PCA. In general, incorporating PCA as an initial preprocessing step has been shown to enhance accurate retrieval and improve the performance of classifiers,

especially for algorithms that rely on linear separation or probabilistic modeling, table 6 summarizes the most important results obtained from the scientific paper.

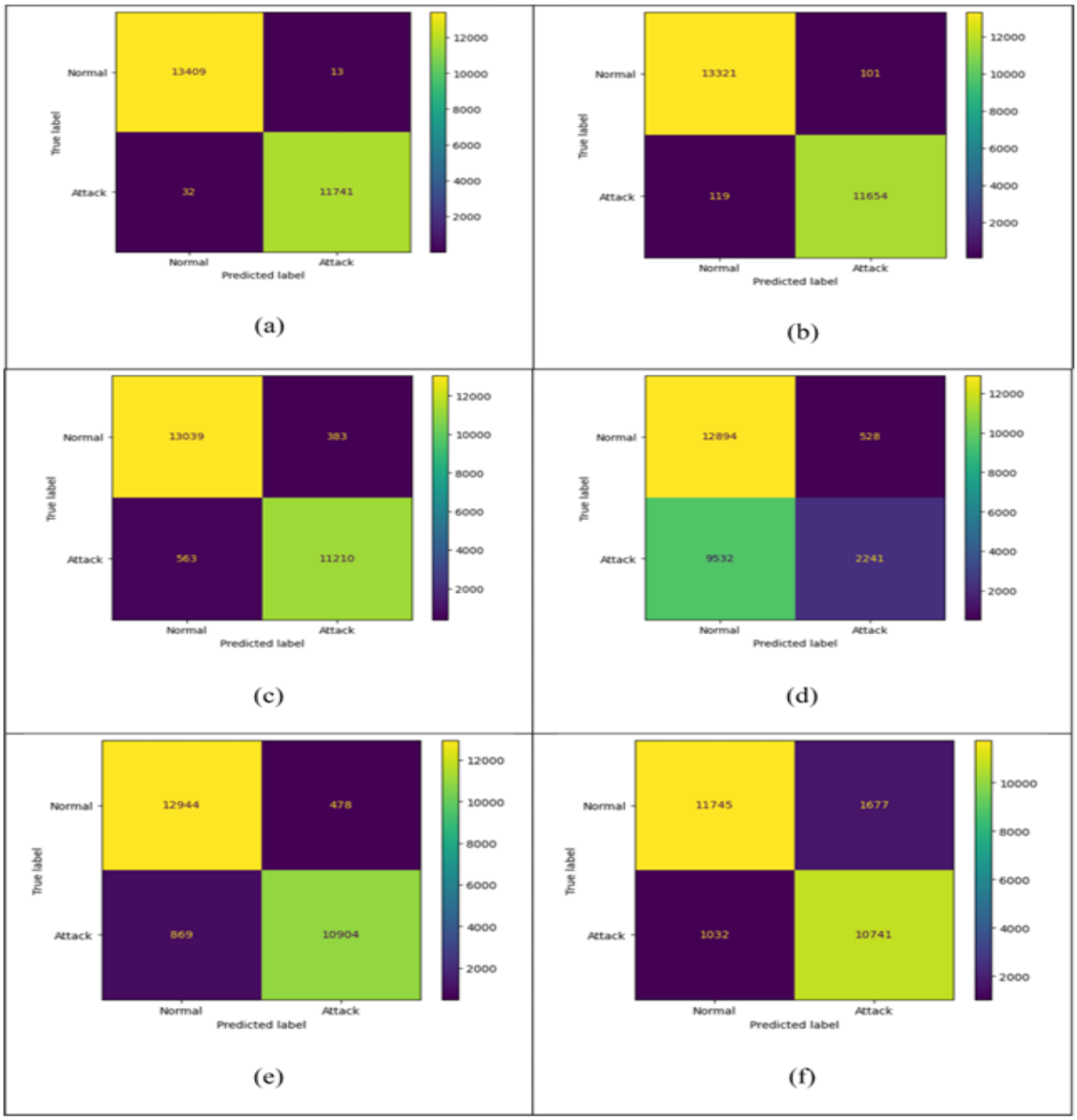


Fig. 10. Confusion matrix without using PCA.

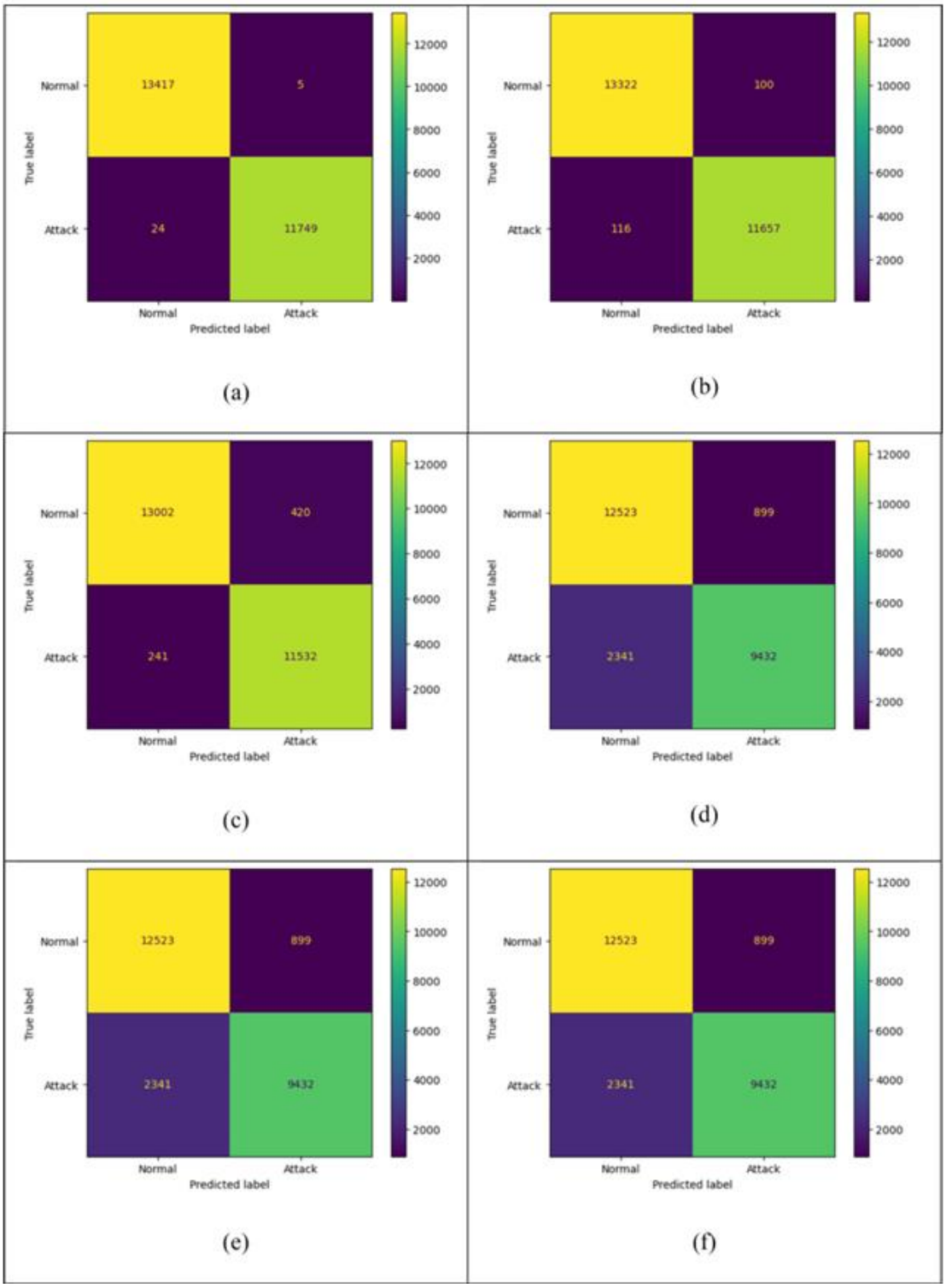


Fig.11. Confusion matrix using PCA.

Table 6

Classifier	Without PCA: Precision, Recall, F1-Score, Accuracy, Kappa	With PCA: Precision, Recall, F1-Score, Accuracy, Kappa
Random Forest	**HIGH**	**HIGH**
K-Nearest Neighbour	**MODERATE**	**MODERATE**
Decision Tree	**REASONABLE**	**REASONABLE**
Support Vector Machines	**MODERATE**	**LOWER**
Logistic Regression	**MODERATE**	**LOWER**
Naïve Bayes	**LOW**	**LOWER**

5. Conclusion

Researchers in [5] found that machine learning classifiers whose work focused on detecting Distributed Denial of Service (DDoS) attacks on IoT devices were highlighted in six different classifiers including Random Forest, Naïve Bayes, K-Nearest Neighbor, and Decision Tree. Random Forest in particular, combined with PCA, is effective in identifying DDoS attacks on IoT devices, highlighting its capabilities in cybersecurity applications. The researchers noted that Naïve Bayes classifiers showed relatively poor performance. K-Nearest Neighbor and Decision Tree classifiers showed strong results.

One of the most important results was observed by researchers in the work [1] where the DeepDefend framework was presented as an innovative solution to detect DDoS attacks and work to mitigate their effects in cloud systems. The DeepDefend framework proved to be highly effective in detecting DDoS attacks by working to concentrate computational power. During critical moments when DDoS attacks occur, which represents only 0.31% of the total monitoring time, early detection of attacks by predicting entropy in online systems and addressing and improving challenges with scalability in cloud systems. Also note that the proposed method of the DeepDefend framework works to optimize resources by focusing on the important moments of attacks, which reduces the burden on the system’s resources compared to traditional detection methods.

https://scopmajd.com/ « ISI: (0.841) « ISSN (Online): 3005-2033

REFERENCES

1) Afdel, K; Agherrabi, E; Akouhar, M. (2024). DeepDefend: A comprehensive framework for DDoS attack detection and prevention in cloud computing, Journal of King Saud University-Computer and Information Sciences: 36(3): 2-25.
2) Alamgir Hossain, A; Islam, S. (2024). Enhancing DDoS attack detection with hybrid feature selection and ensemble-based classifier: A promising solution for robust cybersecurity, Measurement: Sensors 32(5): 12-25.
3) Javanmardi, S Meysam Ghahramani, M. Mohammad Shojafar, M; Alazab, F. (2024). M-RL: A mobility and impersonation-aware IDS for DDoS UDP flooding attacks in IoT-Fog networks, Contents lists available at ScienceDirect 140(3): 1-13.
4) Nalayini C.M; Geetha S. b L Eunaicy J.I. (2024). A novel dual optimized IDS to detect DDoS attack in SDN using hyper tuned RFE and deep grid network. Cyber Security and Applications 2(76). 21-35.
5) Sanjit Kumar, S; Mahapatra, S Mohant, N; Gupta, M. (2024). Enhancing DDoS attack detection in IoT using PCA. Egyptian Informatics Journal 25(3): 23-34.
6) Usman Haruna Garba, U; Adel, N; Pasha, M; Khan, S. (2024). SDN-based detection and mitigation of DDoS attacks on smart homes, Journal Pre-proof 24(1): 3-12.