EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Cloud DDoS Attack Detection Model with Data Fusion & Machine Learning Classifiers

Lal Mohan Pattnaik[1], Pratik Kumar Swain[1], Suneeta Satpathy[2,*] and Aditya N. Panda[1]

[1]Faculty of Emerging Technologies, Sri Sri University, Cuttack, Odisha, India
[2]Center for AI & ML, SOA University, Bhubaneswar, Odisha, India

Abstract

In the current situation, digital technology is a necessary component of daily life for people. During the Covid-19 pandemic, every profit and non-profit making businesses organizations moved online, which caused an exponential rise in incursions and attacks on the digital platform. The Distributed Denial of Service (DDoS) attack, which may quickly paralyse Internet-based services and applications, is one of the deadly threats to emerge. The attackers regularly update their skill tactics, which allows them to get around the current detection and protection systems. The standard detection systems are ineffective for identifying novel DDoS attacks since the volume of data generated and stored has multiplied. So, the main goal of this work is to employ data fusion applications for secure cloud services and demonstrate the detection of DDoS attacks with the applications of machine learning classifiers that can further be helpful for cloud forensic investigation process. A variety of machine learning models, including decision trees, Navies Bayes, SVM, and KNN are used to detect and classify cloud DDoS attacks. The outcomes of the experiments demonstrated that decision tree is the most feasible and better performer method to classify cloud DDoS attacks.

Keywords: Cloud Security, DDoS, Machine Learning, Data Fusion

Received on 14 June 2023, accepted on 27 August 2023, published on 21 September 2023

doi: 10.4108/eetsis.3936

1. Introduction

Cloud computing is a resource that allows clients to use resources like web servers, database, storage services and application services over the internet either in free of cost or pay-per-use basis without investing and maintaining physical hardware and software infrastructure. Cloud computing enables organizations and individuals to scale their computing resources up or down as needed, depending on their workload requirements. Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) are the three main cloud computing services. IaaS offers services including web servers, storage, and networking in addition to computational capabilities.

*Corresponding author. Email: suneeta1912@gmail.com

PaaS provides a better platform for developers for building and managing their applications without any adverse effect. SaaS provide access to applications software like email, software tools, etc. over the internet to the clients. Cloud Computing is gaining popularity in business and personal use day by day due to the notable benefits like scalability, cost savings, flexibility, reliability, security etc. Along with the benefits cloud services also brings no of disadvantages like dependency on Internet Connectivity, Limited Control, Data Security Concerns, Privacy Concerns and cost. So, cloud security is needed to protect user data and prevent unauthorized access, data breaches, and cyber-attacks in the cloud computing environment. Cloud computing involves storing and accessing data over the internet, which can increase the risk of security threats. There are many reasons to justify the need of cloud security as follows [1].

1.1. Data Privacy

Cloud security measures help ensure the privacy of user data in the cloud, protecting sensitive information from unauthorized access.

1.2. Compliance

Organizations are often subject to regulatory compliance requirements, and cloud security helps them meet these requirements.

1.3. Threats

Cyber-attacks and data breaches are a constant threat to organizations using the cloud, and cloud security measures help mitigate these risks.

1.4. Data Loss

Cloud security measures can help prevent data loss due to hardware or software failure, accidental deletion, or other disasters.

1.5. Reputation

A data breach or cyber-attack can damage an organization's reputation, and cloud security measures help protect against such incidents.

1.6. Legal Issues

Organizations can face legal issues if their data is not properly protected in the cloud, and cloud security measures can help prevent such issues.

Overall, cloud security is critical to ensuring the safety and privacy of user data in the cloud, and to mitigating the risks of cyber-attacks, data breaches, and other security threats.
The rest of the paper is organized as follows: Section 2 gives an overview of cloud computing threats followed by detail explanation of DDoS. The related work on DDoS is briefed in section 3 followed by outlining the limitations of the literature review. Section 4 emerges with the challenges faced in cloud security and frames a fusion based cloud detection model adapted from JDL data fusion model [2]. Further the model necessitates the application of machine learning for DDoS detection in section 5. Finally, section 6 ends with the concluding remarks and future directions.

2. Cloud Computing Threats and Problem Statement

Security threats are the risks or dangers generated from many sources, including external threats, insider threats, and accidental actions that can break the confidentiality, integrity, & availability (CIA Triad) of the data or information. The security threats can be summed up in figure 1.

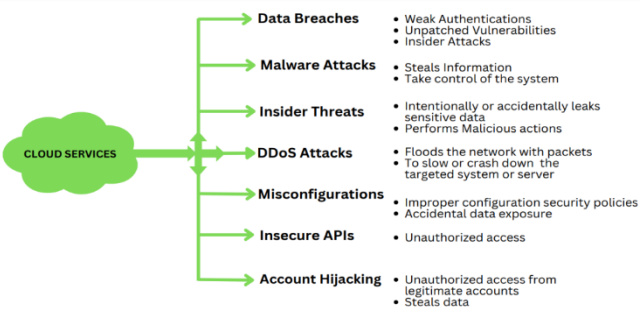

Figure 1. Cloud computing threats

Overall, cloud security threats are a significant concern for organizations using cloud services. The most frequent attack types include DDoS, SYN flood, man-in-the-cloud, flooding, injection, and flooding [3]. One of the largest obstacles to cloud computing security is the distributed denial of service (DDoS) attack, which seeks to overwhelm a system and prohibit users from accessing the services. This kind of assault seriously harm cloud computing infrastructure and prevent authorized customers from using cloud services [4].

A DDoS attack is a type of cyberattack [5] in which one or more attackers commandeer a network of compromised computers, or "botnets," by infecting them with malware or other harmful software. These devices are then used to send a large amount of traffic to the target system or network, essentially clogging up the pipes and preventing legitimate traffic from getting through. DDoS attacks can be carried out for a variety of reasons, such as hacktivism, financial gain, or simply for the thrill of making chaos. They can be difficult to defend against, as they can involve a large number of devices spread across the internet, making it hard to identify and stop the attack.

The attack mechanism of a DDoS attack typically involves four main components: the attacker, handlers, the compromised devices or "botnets," and the target system or network. Attacker usually communicates with bots by using handlers to form a Botnet. The mechanism of DDoS attack is shown in figure 2.

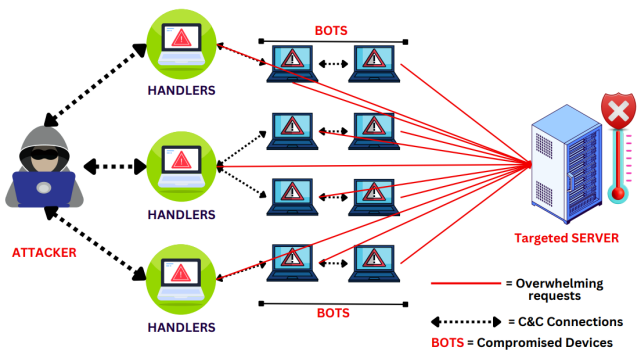

Figure 2. Attack Mechanism of DDoS attack

The taxonomy of DDoS threats is shown in figure 3.

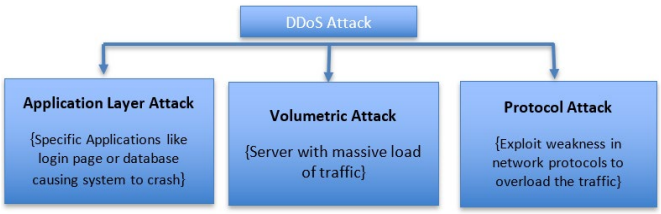

Figure 3. Taxonomy of DDoS attacks

So, the present study concludes that DDoS attacks can be very damaging to the organizations, as it can cause significant downtime, lost revenues, damage reputation. As a line of preventive, it is important for an organization to have best security mechanism in place to defend against DDoS attacks, including intrusion prevention systems, firewalls, and traffic filtering tools.

3. Related work done

A number of papers on DDoS defensive techniques for cloud computing directly relevant to our topic are included in the literature survey. A limited number of authors have focused on identifying and mitigating Distributed Denial of Service (DDoS) attacks, while some research studies have also attempted to evaluate the methods used for detecting such attacks. The objective of the current study is to create a machine learning classification algorithm-based fusion-based cloud DDoS detection model for DDoS attack detection and mitigation. At the same time, Table 1's detailed literature review proposes the real problem for a cloud DDoS attack detection and mitigation model**.**

Table 1. Literature Review

Author & Year	Work Done
F. Musumeci et.al (2022) [6]	They investigated the potential of AI&ML algorithms to perform automated detection for DDoS attack. Their results showed 98% above in accuracy, precision, recall and F1-score.
Z. Liu et.al (2022) [7]	They used machine learning to detect DDoS attacks, and their findings indicated that the linear SVM model outperforms the logistic regression model on the DDoS Evaluation Dataset (CIC-DDoS2019).
U. Islam et.al (2022) [8]	They worked on detection of DDoS Attacks in Banking Sector using ML Model, they implemented machine learning algorithms like SVM, KNN & RF. Each algorithm performed with 99.5%, 97.5%, and 98.74% accuracy, respectively, for the detection of DDOS attacks.
Sumathi S et.al (2021) [9]	Using the CAIDA dataset and ML technique, they focused on the TCP Flood DoS attack detection. Their findings demonstrated that the False Positive Rate, precision, recall, and F-measure had respective values of 0.05, 0.93, 0.95, and 0.91.
Sudar K M et.al (2021) [10]	They implemented machine learning technique namely Decision Tree and Support Vector Machine (SVM) to detect malicious traffic. Their results shows that the Decision Tree and Support Vector Machine (SVM) algorithm provides better accuracy and detection rate.
G. Lucky et.al (2020) [11]	They worked on detection of DDoS attacks using KNN, and the result showed 97.83% accuracy.
Saini et.al (2020) [12]	They proposed RF-based method for classification of DDoS attacks as Benign or Non-Benign. Their results showed that RF method was 198% more effective in detection.
Bagya Lakshmi C et.al (2020) [13]	For DDoS detection, they worked on these ML algorithms of NB, SVM, and DT using feature selection techniques. According to their findings, LVQ picked 20 of the 42 features, whereas PCA identified 21 features. In comparison to other algorithms, DT was the most accurate.
A. R. Wani et.al (2019) [14]	They used Tor Hammer as an attacking tool while working in their own cloud environment, and IDS was used to create a new dataset. Their classification accuracy after applying different ML algorithms, including SVM, NB, and RF, was 99.7%, 97.6%, and 98.0%, respectively.
J. Ye et.al (2018) [15]	They work on the detection of DDoS attack in SDN. Their results showed that average accuracy rate of their method is 95.24%.
Khuphiran P. et.al (2018) [16]	They worked on traditional SVM and DL algorithm named DFF using DARPA 2009 Dataset. Their results showed accuracy of 99.63% in TT of 289.614s for DFF & For SVM, the highest accuracy achieved is 93.01%, in TT of 371.118 secs.
N. A. Putri et.al (2018) [17]	They worked on DoS attack detection using KNN algorithm using ISCX Dataset. Their result showed the accuracy of the KNN algorithm of 97,83%, to its rate of detection 98,63%, and the false alarm was 0.02%.
M. Zekri et.al (2017) [18]	On the basis of the DT, NB, and KNN algorithms, they designed a DDoS detection system. The accuracy of their results was 98.8%, 91.4%, and 95.9%, respectively.

Kumari K. et.al (2022) [19]	They worked on DoS attack detection using LR & NB algorithm. Their results showed the accuracy of 99%-100% (LR) & 99% -98% (NB).
Amrish et.al (2022) [20]	They worked on DDoS attack detection using ANN, KNN, RF & DT using CICDDoS2019 dataset. Their results showed that out of 88 features 15 best features were extracted & ANN outperformed these 3 algorithms with an accuracy of 99.95%.
C M Nalayinil et.al (2022) [21]	They worked on detection of DDoS attack using LR, RF, KNN, NB, DT & SVM. They used the CICIDS2017 Dataset, results showed that RF outperformed all algorithm with an accuracy of 99.885%, 99.88% Precision, 100% Recall & 0.05% False alarm rate.
Alduailij et.al (2022) [22]	They used MI and RFFI to work on ML-based DDoS attack detection. They used RF, GB, WVE, KNN, and LR, and the accuracy of RF, GB, WVE, and KNN with 19 characteristics was 0.99, according to the results.
Sumathi et.al (2022) [23]	They focused on IDS models based on ML to detect DDoS attacks. They used C4.5, SVM, and KNN. Their findings demonstrated that the C4.5 and SVM combination outperformed all other models with an accuracy of 0.9604.
Ashutosh Nath Rimal et.al (2020) [24]	They worked on DDoS attack detection using SVM & NB algorithms. Their results showed that SVM has greater accuracy than NB. SVM has the highest efficiency of 99.68%.
Mahajan (2017) [25]	They worked on the implementation of ML classifiers for the Detection of DDoS attacks. The overall accuracy of 96.89%, 98.89% and 98.91%, 92.31% for NB, DT, MLP-ANN and SVM respectively was obtained.

The research gaps and limitations in machine learning techniques for detecting DDoS attacks from the existing literature are identified based on the below mentioned limitations.

(i) The majority of research papers have concentrated on analysing ML/DL models in controlled conditions rather than assessing how well they function in scenarios where actual DDoS attacks actually take place. To ensure the practical usability of ML/DL models, research is required to validate their efficacy in real-world contexts.

(ii) DDoS attack patterns are constantly changing and evolving, necessitating ML/DL models that can be updated often to recognize new kinds of attacks. DL models that can adapt and stay up with the dynamic nature of DDoS attacks are currently lacking in the literature.

(iii) The processing power and memory resources of networks like the Internet of Things (IoT), Mobile Ad-hoc Networks (MANETs), and wireless sensor networks are constrained. As a result, in these situations of limited resources, there is a need for lightweight ML/DL models that can effectively detect security vulnerabilities. Future studies should concentrate on creating effective and portable DL models created especially for these network contexts.

(iv) The range of attack types and data quality in the existing datasets used for training and evaluating ML/DL models for DDoS attack detection is frequently lacking. This constraint may result in biased detection systems that are unable to effectively classify all forms of attacks. For the development of more precise and efficient detection models, it is necessary to create and make available a variety of datasets that cover different attack types.

By addressing these research gaps, future studies can contribute to the advancement of ML/DL techniques for detecting DDoS attacks and enhance the overall effectiveness of cybersecurity measures.

4. Proposed Fusion Based Cloud DDoS Detection Model

Cloud service security analysts are encountering a new challenge when it comes to jurisdiction and identifying crimes committed on the internet, which transcend geographical boundaries. To address this, a multilateral approach to analyzing and preventing attacks is required. The analysts must analyze vast amounts of data, but the simultaneous collection and analysis of such large volumes can potentially degrade analysis performance to unacceptable levels. In this context, data fusion becomes crucial as it leverages computer technology to process significant amounts of information quickly.

Multi-sensor data fusion is a new technology that tries to combine data from several sources to produce superior information and more precise environmental assessments. A data fusion system's main goals include ensuring accuracy and comprehensiveness, as well as enhancing the variables that affect performance measurement and reducing information overload.

The research presented a cloud-based DDoS detection model (Figure 4) that incorporates data fusion techniques. The model groups and merges data fusion activities or processes that yield the same output into relevant phases. This grouping process helps balance the detection and analysis processes, resulting in higher-quality data for analysis. The proposed model draws inspiration from data fusion models that integrate data from diverse and heterogeneous sources to

achieve high threat detection rates while minimizing false alarm rates.

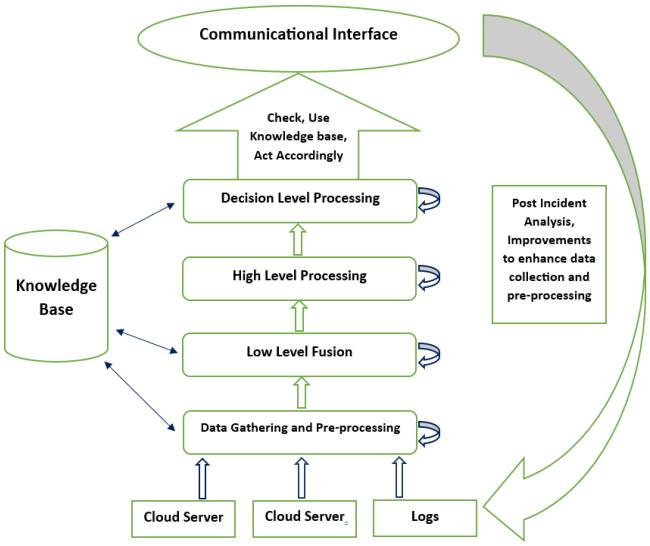

Figure 4. Fusion based Cloud DDoS Detection Model Adapted from [26]

The researchers in proposed a fusion based digital investigation model by grouping and merging one or more activities of digital investigation into data fusion labels. The model is also used for computer forensic investigation of internet uses of the employees in the organization.

The phases of fusion based cloud DDoS detection model can be described as follows.

4.1. Cloud Space

These represent the sources acknowledged by the cloud service providers from which the data can be collected for analysis with an intention to evaluate and measure the intent, lethality of cloud threats.

4.2. Data Gathering & Pre-Processing

The preliminary step of inspection, evaluation in data fusion-based detection model is to gather data and progress it so that data can be aligned into a common format for further analysis. The alignment can be done on the basis of specific features chosen for evaluation and detection process. The processed outcome of this phase can be saved into the knowledge base so that it can be used in the upper part of fusion and mining steps for cloud threat prediction and mitigation.

4.3. Knowledge Base

It is the storage repository of useful features and their respective domain values for measuring and predicting cloud threats. The knowledge base is useful for timely, accurate recommendation, detection and prediction and evidence of further future cloud threat detection, prevention and evaluation.

4.4. Low level fusion

This stage of fusion process along with machine learning techniques can be used for further data clean up, transformation, alteration, domain of data attenuation. It can lessen the voluminous data that has come up in cloud Space and there by advances the cloud data for further eminence with bare minimum loss of aspect.

4.5. High-level fusion

In this phase the correlation between features for detecting, predicting and mitigating the cloud threats are established. Such establishment of association between the filtered features under detection can include clustering, classification, association. The results of such analysis would be indicative of critical feature outlines of cloud threats. Such identification, classification and recognition of cloud threat levels can be effectively extended for further cloud threat detection, prediction as well as mitigation.

4.6. Decision level Processing

The useful outlines obtained from the previous level of fusion are required to be analyzed by the security analysts at different levels to obtain justification of their detection and further analysis. This level of fusion focuses on finding out threat level so that further course of action needs to be followed to enhance detection and prevention process.

The report of this phase can be generated as a threat analysis report for cloud threats as an evidential report for law enforcements and investigating agencies.

4.7. Communicational Interface

The Communicational interface is a medium of interaction between the Fusion based detection and prediction model and with the security analyst groups for better post mortem analysis which can further be used by investigative agencies to provide the steps of prevention and propose the guidelines to be followed by the consumers and service providers in order to maintain discipline of the cloud space.

5. Exploring Data Fusion and Machine Learning for Cloud DDoS detection

The fusion-based cloud DDoS detection model introduced in this research addresses the detection process by generating an optimal feature set. This is achieved by fusing features from various sources obtained from datasets. Additionally, the study aims to leverage machine learning techniques for the identification and mitigation of DDoS attacks within a cloud

environment. From a total of 88 features, 15 features are selected based on their correlation values. These selected features are then trained using four machine learning algorithms for the classification of DDoS attacks. The implementation of this approach utilizes the Python programming language.

5.1. Cloud Space (Data Set)

CICDDoS2019dataset(https://www.unb.ca/cic/datasets/ddos2019.html,http://205.174.165.80/CICDataset/CICDDoS2019/Dataset/CSVs/) have been implemented in our research paper. The dataset used in the study consists of a standardized set of data that includes DDoS threats. It comprises a total of 88 features, with 15 features specifically addressing DDoS traffic input, while the remaining two features represent the label indicating whether the data is benign or nonbenign.

The size of the dataset contains 5074413 rows and 88 columns, this dataset encompasses all DDoS attack types and has been utilized by multiple researchers in machine learning algorithms. It includes a range of DDoS attack classes, covering the following:

(i). DDoS_DNS
(ii). DDoS_MSSQL
(iii). DDoS_UDP

The data set is presented in the following summarized schema in figure 5.

	Unnamed: 0	Flow ID	Source IP	Source Port	Destination IP	Destination Port	Protocol	Timestamp	Flow Duration	Total Fwd Packets	...	Active Std	Active Max	Active Min	Idle Mean
0	425	172.16.0.5-192.168.50.1-634-60495-17	172.16.0.5	634	192.168.50.1	60495	17	2018-12-01 10:51:39.813448	28415	97	...	0.0	0.0	0.0	0.0
1	430	172.16.0.5-192.168.50.1-60495-634-17	192.168.50.1	634	172.16.0.5	60495	17	2018-12-01 10:51:39.820842	2	2	...	0.0	0.0	0.0	0.0
2	1654	172.16.0.5-192.168.50.1-634-46391-17	172.16.0.5	634	192.168.50.1	46391	17	2018-12-01 10:51:39.852499	48549	200	...	0.0	0.0	0.0	0.0
3	2927	172.16.0.5-192.168.50.1-634-11894-17	172.16.0.5	634	192.168.50.1	11894	17	2018-12-01 10:51:39.890213	48337	200	...	0.0	0.0	0.0	0.0
4	694	172.16.0.5-192.168.50.1-634-27878-17	172.16.0.5	634	192.168.50.1	27878	17	2018-12-01 10:51:39.941151	32026	200	...	0.0	0.0	0.0	0.0
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
5074408	6364	172.16.0.5-192.168.50.1-900-23579-17	172.16.0.5	900	192.168.50.1	23579	17	2018-12-01 11:22:40.253588	1	2	...	0.0	0.0	0.0	0.0
5074409	5576	172.16.0.5-192.168.50.1-900-54596-17	172.16.0.5	900	192.168.50.1	54596	17	2018-12-01 11:22:40.253659	30	2	...	0.0	0.0	0.0	0.0
5074410	26506	172.16.0.5-192.168.50.1-900-14341-17	172.16.0.5	900	192.168.50.1	14341	17	2018-12-01 11:22:40.253852	1	2	...	0.0	0.0	0.0	0.0
5074411	18736	172.16.0.5-192.168.50.1-900-46229-17	172.16.0.5	900	192.168.50.1	46229	17	2018-12-01 11:22:40.254534	1	2	...	0.0	0.0	0.0	0.0
5074412	2811	172.16.0.5-192.168.50.1-900-23895-17	172.16.0.5	900	192.168.50.1	23895	17	2018-12-01 11:22:40.254719	2	2	...	0.0	0.0	0.0	0.0

Figure 5. CIC-DDoS2019(DNS) Dataset

5.2. Data gathering and Pre-processing

In the proposed DDoS attack detection model, data pre-processing plays a critical role as it involves the analysis and transformation of raw data into the desired format shown in fig.5. This step is crucial as it sets the foundation for subsequent analysis and is considered the most significant step in the process.

5.3. Low Level Fusion

In this step, Null values that interpret all required analysis steps, including plotting and model fitting, are eliminated. Therefore, the data's null values are eliminated using dropna() because they may be misleading for DDoS attack detection. So the dataset which was 5074413 rows × 88 columns and after the command dropna() the dataset becomes 5073181 rows × 88 . In addition, the data pre-processing step includes feature selection based on correlation values. The correlation value of a feature is typically calculated by assessing its relationship with the target variable. Correlation helps evaluate the strength and direction of a linear relationship between multiple variables.

5.4. High Level Fusion

The entire dataset is then divided in half at a ratio of 70:30, with 70% of the data designated for training and the remaining 30% set aside for testing. The extracted features from the dataset are then used to train a machine learning classification algorithm. The process of machine learning involves the use of mathematical algorithms, statistical models, and computer algorithms to automatically improve the accuracy of predictions over time. The algorithm learns from past data, detects patterns and makes predictions based on that.

5.5. Decision Level Fusion

Artificial intelligence is used in machine learning, which focuses on creating algorithms that can recognize patterns in data and predict outcomes without being explicitly programmed. It involves training computer programs to automatically recognize and make predictions on patterns in data.
The following Machine Learning algorithms are used for detection and classification of DDoS datasets:

(i) Decision Tree (DT): A decision tree employs a tree-like representation of choices and potential outcomes, such as utility and resource costs.
(ii) Naive Bayes (NB): The assumption behind Naive Bayes is that the presence of one feature in a class is independent to the presence of another feature, according to Bayes' theorem.
(iii) K-Nearest Neighbor (KNN): For classification and regression problems, the k-nearest neighbors (KNN) technique is employed. In order to create predictions, it locates the K training dataset data points that are the closest to the new data point.
(iv) Support Vector Machine (SVM): Regression analysis and classification both employ SVM (Support Vector Machine). It locates the most effective hyperplane for classifying data.

Below are the performance measurement metrics commonly used for comparing machine learning algorithms:

(i) Accuracy: It displays the proportion of correctly identified observations among all observations.
Accuracy = (TP + TN) / (TP + TN + FP + FN)

(ii) Precision: In relation to all predicted positive observations, it calculates the proportion of correctly predicted positive observations.
Precision = TP / (FP + TP)

(iii) Recall: Out of all positive observations, it represents the proportion of accurately predicted positive observations.
Recall = TP / (FN + TP)

(iv) F1-score: It measures the harmonic mean, which takes into account both false positives and false negatives, between precision and recall.
F1-score = 2 * TP / (2 * TP + FN + FP)

By evaluating the accuracy, precision, recall, and overall classification skills of machine learning algorithms, these measures offer insightful information about how well they function.

Figure 6 depicts the performance metrics values of DT, NB, SVM and KNN. Table 2 makes a Comparative analysis of Various Parameters of the Different classifier algorithms.

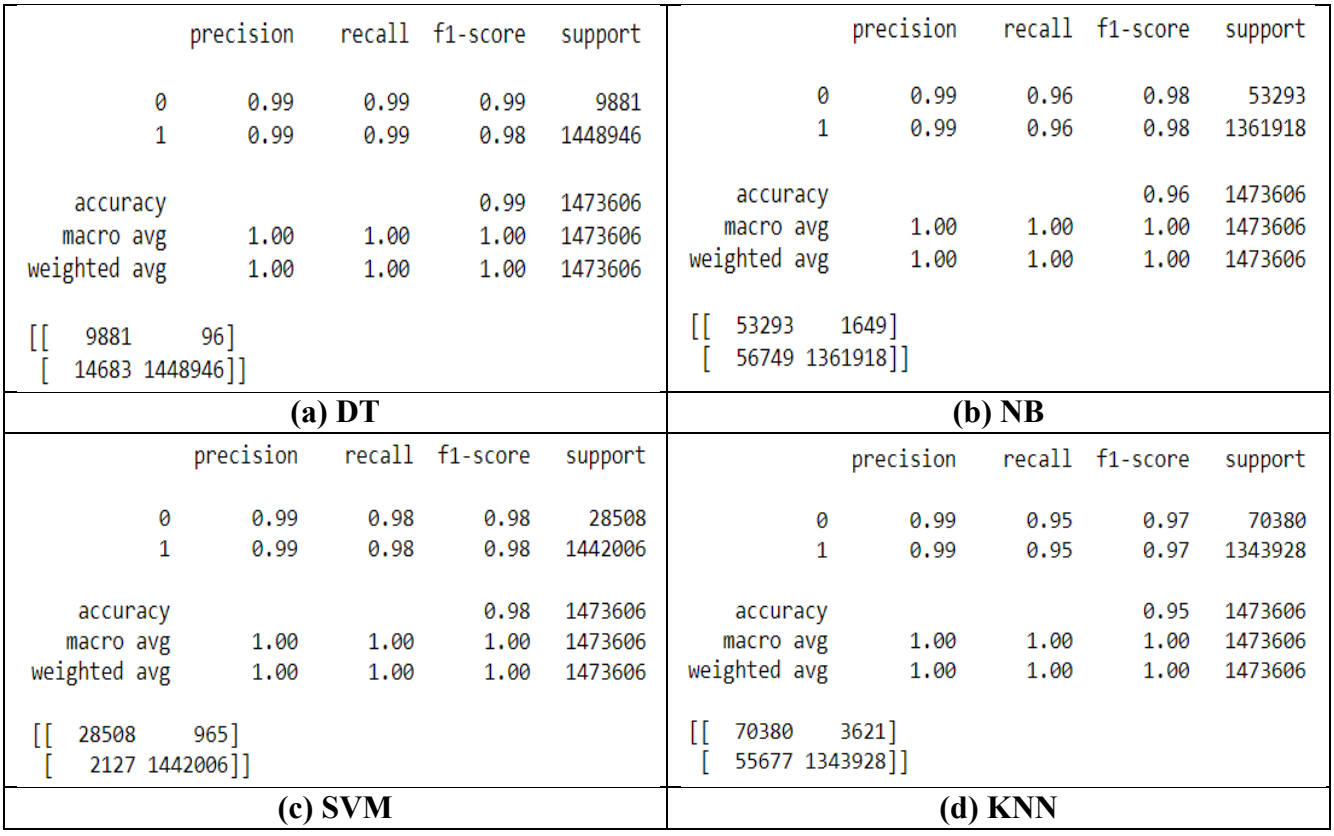

Figure 6. The performance metrics values of (a)DT, (b)NB, (c)SVM and (d)KNN

Table 2. Comparative Analysis of Classification Algorithms Based on Various Parameters.

ML	TP	TN	FP	FN
DT	1448946	14683	96	9881
NB	1361918	56746	1649	53293
KNN	1343928	55677	3621	70380
SVM	1442006	2127	965	28508

The results of the simulation for various classification models are presented in Table 3.

Table 3. Comparative Analysis of Classification Performance comparison of different machine learning classifies.

ML	Accuracy (%)	Precision (%)	Recall (%)	F1 (%)
DT	99%	99%	99%	99%
NB	96%	99%	96%	98%
KNN	95%	99%	95%	97%
SVM	98%	99%	98%	98%

In conclusion, the research study found that the Decision Tree (DT) model exhibited the highest performance, achieving an accuracy score of 99%. The study focused on the CIC-DDoS2019 dataset, which consists of 88 features, from which the top 15 features were extracted. To establish the best classifier for a fusion-based DDoS detection model, this study is utilizing four different algorithms, including NB, KNN, SVM, and DT. The results indicated that the Decision Tree classifier outperformed the other models, achieving an impressive accuracy of 99%.

6. Conclusions and Future Work

The research study aimed to detect DDoS attacks on cloud computing platforms by employing various machine learning algorithms. To achieve this, a fusion-based DDoS attack detection model was proposed, which extracted actionable characteristics and distinguished different types of attacks. Recognizing the dynamic nature of DDoS attacks, it was crucial to collaborate and correlate data from cloud spaces and unique platforms. As a potential extension of the current work, merging multiple classifiers could lead to improved performance.

Additionally, the proposed model could be extended to assist law enforcement and investigating agencies in tracing the origins of attacks and identifying the attackers. Given the increasing complexity of attack techniques, future research could focus on enhancing cloud computing attack detection through automated fusion applications and optimized algorithms. Furthermore, exploring different feature selection techniques and incorporating various types of modern attacks in cloud services should be considered in future work.

References

[1] Garima and S. J. Quraishi, "Machine Learning Approach for Cloud Computing Security," *2022 3rd International Conference on Intelligent Engineering and Management (ICIEM)*, London, United Kingdom pp. 158-163, (2022) doi: 10.1109/ICIEM54221.2022.9853056.

[2] T. Bass, Multi-sensor Data Fusion for Next Generation Distributed Intrusion Detection System, In Proceedings of the IRIS National Symposium on Sensor and Data Fusion, (1999).

[3] Utsav Vora; Jayleena Mahato; Hrishav Dasgupta; Anand Kumar; Swarup Kr Ghosh, "Machine Learning–Based Security in Cloud Database—A Survey," in *Machine Learning Techniques and Analytics for Cloud Security*, Wiley pp.239-269, (2022) doi: 10.1002/9781119764113.ch12.

[4] Emad Ali, Tariq & Chong, Yung-Wey & Manickam, Selvakumar. Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review. Applied Sciences. 13. 3183. 10.3390/app13053183. (2023)

[5] S. Potluri, M. Mangla, S. Satpathy and S. N. Mohanty, "Detection and Prevention Mechanisms for DDoS Attack in Cloud Computing Environment," 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2020, pp. 1-6, (2020) doi: 10.1109/ICCCNT49239.2020.9225396.

[6] F. Musumeci, A. C. Fidanci, F. Paolucci, F. Cugini, and M. Tornatore, "Machine-Learning-enabled DDoS attacks detection in P4 programmable networks," Journal of Network and Systems Management, vol. 30, no. 1, pp. 1–27(2022) doi: 10.1007/s10922-021-09633-5.

[7] Z. Liu, L. Qian, and S. Tang, "The prediction of DDoS attack by machine learning," in Third International Conference on Electronics and Communication; Network and Computer Technology (ECNCT 2021), pp. 681–686 (2022) doi: 10.1117/12.2628658.

[8] U. Islam et al., "Detection of distributed denial of service (DDoS) attacks in IoT based monitoring system of banking sector using machine learning models," Sustainability, vol. 14, no. 14, p. 8374 (2022) doi: 10.3390/su14148374

[9] Sumathi S & Rajesh R, Comparative study on TCP SYN flood DDoS attack detection: A machine learning algorithm based approach, WSEAS Trans Syst Control, 16(1) 584–591(2021)

[10] Sudar K M, Beulah M, Deepalakshmi P, Nagaraj P & Chinnasamy P, Detection of Distributed Denial of Service Attacks in SDN using Machine learning techniques, in IEEE Int Conf Comput Commun Informat (ICCCI) 1–5 (2021) doi: 10.1109/ICCCI50826.2021.9402517

[11] G. Lucky, F. Jjunju, and A. Marshall, "A lightweight decision-tree algorithm for detecting DDoS flooding attacks," in 2020 IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C) pp. 382–389, (2020), doi: 10.1109/QRS-C51114.2020.00072.

[12] Saini, P. S., Behal, S., & Bhatia, S "Detection of DDoS Attacks using Machine Learning Algorithms". 7th International Conference on Computing for Sustainable Global Development (INDIA.Com).pp;16-21. (2020).

[13] Bagyalakshmi C & Samundeeswari E S, DDoS attack classification on cloud environment using machine learning techniques with different feature selection methods, Int J, 9(5) (2020).

[14] Wani, A. R., Rana, Q. P., Saxena, U., & Pandey, N. Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques. 2019 Amity International Conference on Artificial Intelligence (AICAI). (2019) doi:10.1109/aicai.2019.8701238

[15] J. Ye, X. Cheng, J. Zhu, L. Feng, and L. Song, "A DDoS attack detection method based on SVM in software defined network," Security and Communication Networks, pp. 1–8, 2018, doi: 10.1155/2018/9804061.

[16] Khuphiran P., Leelaprute, P., Uthayopas, P., Ichikawa, K., & Watanakeesuntorn, W. Performance Comparison of Machine Learning Models for DDoS Attacks Detection. 2018 22nd International Computer Science and Engineering Conference (ICSEC) (2018). doi:10.1109/icsec.2018.8712757

[17] N. A. Putri, D. Stiawan, A. Heryanto, T. W. Septian, L. Siregar, and R. Budiarto, "Denial of service attack visualization with clustering using K-means algorithm," in 2017 International Conference on Electrical Engineering and Computer Science (ICECOS), pp. 177–183, (2017) doi: 10.1109/ICECOS.2017.8167129.

[18] M. Zekri, S. El Kafhali, N. Aboutabit, and Y. Saadi, "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, (2017) doi: 10.1109/CloudTech.2017.8284731.

[19] Kumari, K., Mrunalini, M. Detecting Denial of Service attacks using machine learning algorithms. *J Big Data* **9**, 56 (2022). https://doi.org/10.1186/s40537-022-00616-0

[20] Amrish, R., Bavapriyan, K., Gopinaath, V., Jawahar, A. & Kumar, C. V.. DDoS Detection using Machine Learning Techniques. Journal of IoT in Social, Mobile, Analytics, and Cloud, 4(1), 24-32. (2022) doi:10.36548/jismac.2022.1.003

[21] M NALAYINI, C and Katiravan, Jeevaa, Detection of DDoS Attack Using Machine Learning Algorithms www.jetir.org (ISSN-2349-5162) JETIR July 2022, Volume 9, Issue 7, (2022). Available at SSRN: https://ssrn.com/abstract=4173187

[22] Alduailij, M.; Khan, Q.W.; Tahir, M.; Sardaraz, M.; Alduailij, M.; Malik, F. Machine-Learning-Based DDoS Attack Detection Using Mutual Information and Random Forest Feature Importance Method. Symmetry, 14, 1095. (2022) https://doi.org/10.3390/sym14061095

[23] Sumathi, S ; Rajesh, R ; Karthikeyan, N. DDoS Attack Detection Using Hybrid Machine Learning Based IDS Models. Journal of Scientific & Industrial Research.Vol.81,No.03(2022).http://op.niscair.res.in/index.php/JSIR/article/view/58451

[24] Ashutosh Nath Rimal and Raja Praveen, DDOS Attack Detection Using Machine Learning", International Journal of Emerging Technologies and Innovative Research (www.jetir.org | UGC and issn Approved), ISSN:2349-5162, Vol.7, Issue 6, page no. pp185-188 (2020) Available at : http://www.jetir.org/papers/JETIR2006031.pdf

[25] Mahajan, Amit, Ifran Sofi, Vibhakar Mansotra. Machine Learning Techniques used for the Detection and Analysis of Modern Types of DDoS Attacks. International Research Journal of Engineering and Technology (IRJET) Volume: 04 Issue: 06 (2017).

[26] S Satpathy, A Mohapatra, “A data fusion based digital investigation model as an effective forensic tool in the risk assessment and management of cyber security systems”, The 7th international conference on computing, communications and control technologies (2009).