Real-Time Detection Schemes for Memory DoS (M-DoS) Attacks on Cloud Computing Applications

N Reddy Prasad Reddy, Department of CSE, Narayana Engineering College, Gudur.
Dr. V. Sucharita, Professor, Department of CSE, Narayana Engineering College, Gudur.

Abstract

A Malicious DoS (M-DoS) attack is a type of network attack designed to increase system memory and prevent legitimate users from accessing the system. These attacks pose a significant threat in cloud computing environments where resources are shared by many users. M-DoS attacks are difficult to detect and mitigate immediately because they are characterized by many low-level requests and these attacks are difficult to distinguish from real traffic. To overcome this challenge, various in-flight detection methods have been proposed and SVM algorithms have been used for prediction. The data used in this study was collected from various sources and preprocessed to extract features relevant to the research. Additionally, feature selection procedures were performed to identify the most important features for optimal detection. It is worth noting that the accuracy of the SVM algorithm is 95% higher than other methods.

INDEX TERMS *DDOS, MDOS, cloud computing, memory attacks, ML, DL.*

I.INTRODUCTION

One of the most significant threats to cloud security is Memory Denial of Service (M-DoS) attacks. M-DoS attacks the target's memory, making the resources unavailable to legitimate users. These attacks are especially dangerous in cloud computing environments where many users share resources. Therefore, immediate detection and mitigation of M-DoS attacks is crucial to ensure the availability and reliability of cloud services. environment. These solutions are designed to instantly detect M-DoS attacks without high overhead or security breaches. This technology can be divided into two types categories: signature-based detection and non-invasive detection. Signature-based detection is based on identifying specific patterns or characteristics of M-DoS attack strategies, while anomaly-based detection techniques identify benign behaviour that differs from the standard used Record-based look strategy utilized The fingerprinting assault handle is to begin with put away within the hash table. When a modern ask arrives, it compares the unique mark within the hash table and in the event that a coordinate is found, the ask is classified as an M-DoS assault. An case of helplessness location is the utilize of machine learning calculations to analyse the behaviour of demands and recognize unordinary designs.

II. LITERATURE SURVEY

The research landscape on Distributed Denial of Service (DDoS) attack detection showcases various innovative approaches. In one study, an enhanced K-nearest neighbors (KNN) algorithm is proposed for DDoS attack severity analysis. Another research suggests employing fuzzy Q-learning to prevent DDoS attacks in cloud computing. Lucid, a deep learning approach, integrates convolutional and recurrent neural networks for efficient DDoS detection. Machine learning such as Random Forest and Extreme Gradient Boosting are used for accurate DDoS detection in Cyber Physical Production Systems (CPPS).Apache Spark framework, along with decision trees and random forests, aids in identifying DDoS attacks in private cloud environments. Leveraging cloud computing infrastructure, another study utilizes machine learning for scalable DDoS detection and mitigation. Real-time DDoS flood attack monitoring and detection (RTAMD) model, incorporating

random forests and k-nearest neighbors, achieves prompt detection in cloud environments. A bio-inspired anomaly-based detection system called BARTD effectively identifies under-rated App-DDoS attacks. Furthermore, machine learning algorithms such as decision trees and support vector machines enhance DDoS attack identification and mitigation in cloud computing. In the banking sector, IoT-based monitoring systems leverage random forest and knearest neighbors for precise DDoS attack identification. Overall, the integration of diverse machine learning techniques underscores the significance of multi-faceted approaches in bolstering cybersecurity defenses.

III. METHODOLOGY

Distributed Denial of Service (DDoS) attacks have persistently posed a substantial threat to the availability of network services, presenting a formidable challenge to traditional defense strategies. Despite efforts to mitigate these attacks, finding effective solutions has remained elusive. However, the emergence of Software Defined Networking (SDN) offers a promising avenue for addressing DDoS threats. In this context, the paper under discussion presents two novel detection methods specifically designed for SDN environments. The first method capitalizes on analyzing the degree of DDoS attack activity to identify and characterize malicious traffic. By understanding the intensity and patterns of the attack, this approach aims to swiftly pinpoint and respond to DDoS incidents, thereby enhancing network resilience.

The second detection method introduced in the paper employs an advanced application of the KNearest Neighbors (KNN) algorithm within a broader Machine Learning (ML) framework. This method leverages the power of ML to dynamically learn and adapt to evolving DDoS attack patterns. By analyzing network traffic features and employing the KNN algorithm, this approach aims to accurately distinguish between normal and malicious traffic, thereby enabling proactive defense measures. Overall, these two detection methods represent innovative approaches tailored specifically for SDN environments, harnessing the flexibility and programmability offered by SDN to enhance the detection and mitigation of DDoS attacks. Through their combined utilization, network operators can better safeguard their infrastructure and ensure uninterrupted service availability in the face of persistent DDoS threats. Cloud service providers encounter significant security challenges, with Distributed Denial of Service (DDoS) attacks standing out as one of the most pervasive threats. Detecting such attacks promptly is essential for maintaining the security and availability of cloud environments.

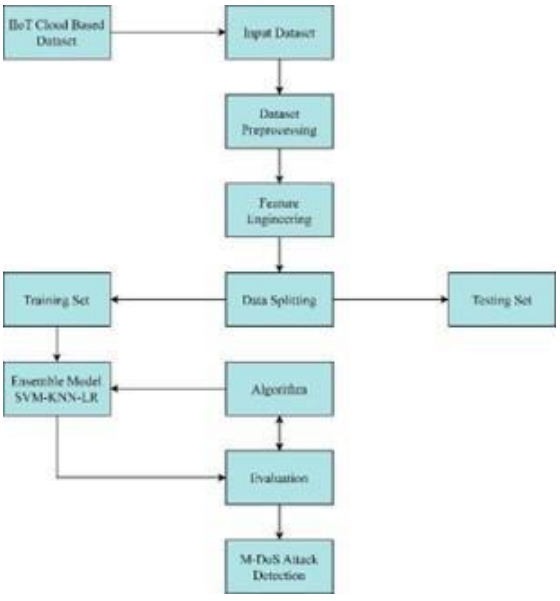


FIG 1. Proposed working flow

This study introduces an innovative approach to address this imperative need for real-time DDoS detection. Leveraging the power of machine learning, the proposed system utilizes advanced classifiers to analyze network traffic patterns and identify potential DDoS attacks as they unfold. To ensure scalability and responsiveness, the detection system is deployed on a distributed processing platform integrated into an OpenStack-based cloud testbed. This environment provides a realistic setting for evaluating the efficacy and performance of the detection mechanisms under diverse network conditions and attack scenarios. Furthermore, the utilization of the Apache Spark framework enhances the efficiency and agility of the detection system. Apache Spark's distributed computing power quickly processes big data on the network, helping detect and respond to DDoS threats in a timely manner. Adaptive defense mechanisms against attacks in the cloud environment. This proactive approach empowers cloud service providers to preemptively mitigate the impact of DDoS attacks, thereby safeguarding the integrity and availability of their services for users and clients.

The banking sector, due to the immense value of its data and critical role in the economy, faces heightened risks from cyberattacks. Among these threats, Distributed Denial of Service (DDoS) attacks pose a significant concern. These attacks, if successful, can disrupt banking services, cause financial losses, and erode customer trust.

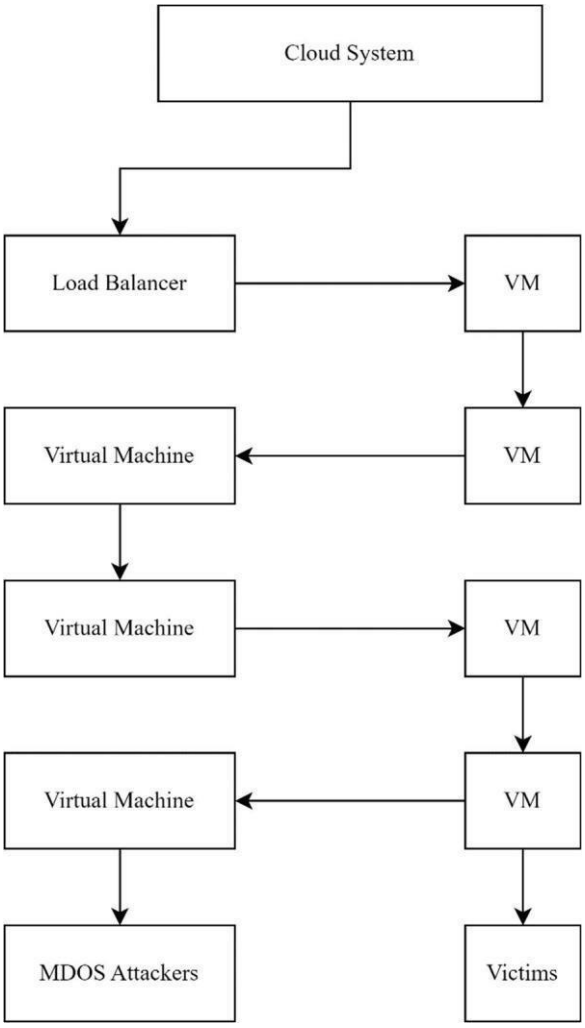
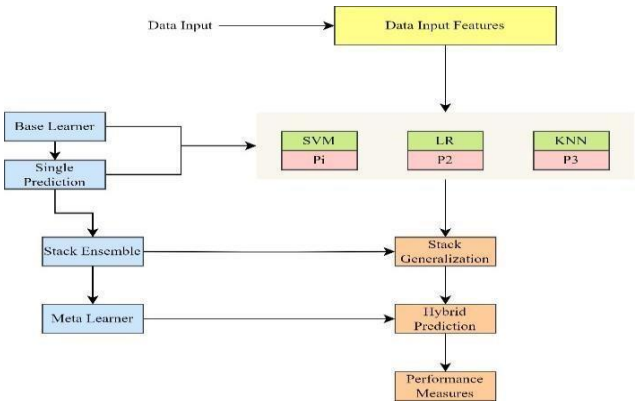


Fig2: Cloud system architecture. Show standard performance of true positives, negatives, negatives and false negatives

This paper directs its attention to mitigating the specific threat of DDoS attacks targeting financial

organizations. To achieve this, the researchers utilize the Banking Dataset, which likely comprises relevant data pertaining to the banking industry's network infrastructure, transactional activity, and other pertinent information. Using this data, the research aims to develop effective methods to detect and mitigate DDoS attacks in the banking sector. Considering the sensitivity of the banking industry and the potential impact of service disruptions, detecting DDoS attacks is critical. Through thorough analysis of the Banking Dataset, the researchers can identify patterns and anomalies indicative of DDoS activity. These insights enable the development of robust detection algorithms and strategies tailored to the unique characteristics of DDoS attacks in the banking domain. By focusing on the Banking Dataset, this paper seeks to enhance the resilience of financial institutions against DDoS threats. Ultimately, the goal is to bolster the security posture of the banking industry, safeguarding critical assets, preserving operational continuity, and upholding trust and confidence among customers and stakeholders. The increasing adoption of Internet of Things (IoT) devices has brought about a host of security challenges, among which Distributed Denial of Service (DDoS) attacks loom large. Given the sheer volume and diversity of IoT devices interconnected within networks, they present a lucrative target for malicious actors seeking to launch large-scale DDoS attacks. To confront this threat, the research leverages the Bot-IoT dataset, which contains valuable insights into the behavior and characteristics of IoT devices, particularly those susceptible to compromise and exploitation by botnets for orchestrating DDoS attacks. One of the key challenges in developing effective intrusion detection systems for IoT environments is the class imbalance problem, wherein the dataset may be skewed towards normal or benign traffic, making it difficult for models to accurately discern anomalous or malicious activity. In response, this research addresses the class imbalance issues inherent in the Bot-IoT dataset. By employing advanced machine learning and deep learning techniques, the study aims to develop an Intrusion Detection System (IDS) capable of effectively identifying and thwarting DDoS attacks targeting IoT devices. These models are trained on the BotIoT dataset to learn complex patterns indicative of malicious behavior, enabling them to distinguish between normal and abnormal traffic with greater accuracy.



Through the utilization of machine learning and deep learning models tailored to the characteristics of IoT environments, this research seeks to enhance the security posture of IoT deployments and mitigate the risk posed by DDoS attacks. By proactively detecting and mitigating such threats, the Intrusion Detection System developed in this study contributes to the protection of IoT ecosystems, safeguarding the integrity, availability, and reliability of IoT services and applications.

Memory-based denial-of-service (DoS) attacks pose a significant threat to the performance and availability of cloud-based applications, particularly those running on co-located virtual machines. This paper conducts experiments to investigate the impact of memory DoS attacks on diverse cloud-based applications. By subjecting these applications to simulated memory-based DoS attacks, the researchers aim to quantify the extent of performance degradation and identify vulnerabilities in cloud environments. The experimental results provide valuable insights into the effects of memory DoS attacks on various aspects of application performance, such as response time, throughput, and

resource utilization. By analyzing these effects across different types of cloud-based applications, the study sheds light on the diverse ways in which memory DoS attacks can disrupt and degrade service delivery in cloud environments. Furthermore, the paper proposes two innovative Statistical-based Detection Schemes (SDS/B and SDS/P) designed to accurately detect memory DoS attacks in real-time. These detection schemes leverage statistical analysis techniques to monitor and analyze system-level metrics and behavior patterns indicative of memory-based DoS attacks. By focusing on lightweight and responsive detection mechanisms, the proposed schemes aim to minimize detection delay and performance overhead, ensuring timely and effective mitigation of memory DoS attacks. Overall, this research contributes to the advancement of security measures in cloud computing by enhancing the detection and mitigation capabilities against memory-based DoS attacks. By combining empirical experimentation with the development of novel detection schemes, the paper provides practical insights and solutions to safeguard cloud-based applications against this pervasive and disruptive threat. This study focuses on the analysis of Mirai, a notorious malware known for creating IoT botnets, which represent a significant threat to cybersecurity. To better understand Mirai's behavior and impact, the researchers undertake a comprehensive examination of its code. By dissecting Mirai's code, the study aims to uncover its mechanisms, functionalities, and vulnerabilities, thereby enhancing our understanding of how it operates and spreads across IoT devices. Moreover, the research endeavors to create a low-cost simulation environment conducive to dynamic analysis of Mirai. This simulation environment serves as a controlled setting where researchers can observe Mirai's behavior under various conditions, facilitating the development of effective countermeasures and mitigation strategies.

In addition to analyzing Mirai's code and simulation, the study conducts controlled DenialofService (DoS) attacks to assess their impact on both compromised and victim IoT devices. By measuring resource consumption metrics such as energy, CPU usage, memory utilization, Ethernet performance, and Secure Digital card usage, the researchers gain insights into the efficiency and effectiveness of Mirai's attack methods. This empirical analysis helps quantify the extent of damage caused by Mirai-infected botnets and informs strategies for mitigating their impact on IoT ecosystems. Overall, this study contributes valuable insights into the behavior and impact of Mirai malware, offering a deeper understanding of its operation and potential consequences. By conducting comparative analyses with previous studies, the research aims to identify trends, patterns, and areas for improvement in cybersecurity defenses against IoT botnets like Mirai. Through this comprehensive approach, the study endeavors to bolster the resilience of IoT networks and devices against evolving cyber threats.

IV. RESULTS AND DISCUSSIONS

The Presentation and Discussion section aims to provide an in-depth study of the results and analysis of the proposed hybrid model incorporating SVM-KNN-LR for M-DoS attack cloud detection in cloudy weather. In this area, the test comes about gotten by assessing the execution of the demonstrate are carefully analyzed. The most objective is to assess the viability of the proposed show in terms of discovery precision, wrong positives, and framework overhead. Moreover, the extent of tests falling exterior the prescribed test for all comes about was compared and analyzed with existing strategies to demonstrate the prevalence of the arranged test. An understanding of the optimization of the proposed demonstrate in a reasonable cloud computing environment will be given. In our think about, the demonstrate was initialized utilizing the broadly utilized Xavier/Glorot initialization, which may be a well known procedure for initialization weights in machine learning models. Agreeing to the dispersion extend, we aim to disperse organize information to the initial or MDoS assault. Utilizing directed learning method, the show is prepared utilizing recorded information. For the activation work, we select the ReLU (Amended Direct Unit) actuation work within the covered up prepare, which is considered as the overshoot prepare.

A. Experiments

This section provides an overview of the experimental setup and methodology used to evaluate the effectiveness of the proposed model in detecting cloud and M-DoS attacks. The experiment is divided into four main phases: data collection, preliminary preparation, model training, and performance evaluation.

Data collection

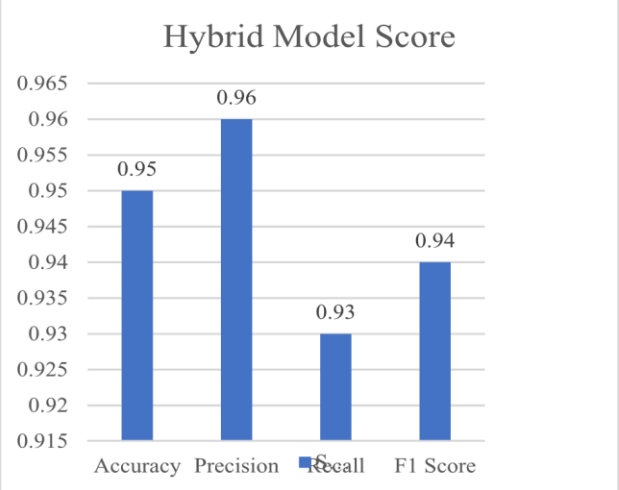
The experimental data used in this study were collected from a real network environment. This file contains network connection data captured during the specified period, including both normal and attack. Data collection techniques include the use of network monitoring tools to capture and record packet traffic on the network. Cybersecurity experts then aggregate the captured data and analyze events related to various types of attacks, including cloud attacks and M-DoS attacks.

Preprocessing

Data preprocessing consists of several simple steps to ensure data quality and suitability for machine learning. Initially, unnecessary data was removed from the dataset to simplify the data for further analysis. After that, pre-processing will transform the dataset into a model optimized for machine learning algorithms. This change involves cleaning the data by removing irrelevant or irrelevant material that may distort the truth. An important part of data cleaning is the removal of missing values, which is done by replacing null values (such as NaN values) with zeros. Additionally, the preprocessing phase needs to remove duplicate values and resolve other anomalies present in the dataset. By solving these problems, data becomes more efficient and machine learning becomes easier to analyze accurately.

Training model

The preparing show combines back vector machine (SVM), k-nearest neighbor (KNN) and calculated relapse (LR) and is to begin with prepared utilizing the information content. Amid preparing, information is more often than not part between preparing and testing in a 70:30 or 80:20 proportion. The preparing strategy is utilized to prepare the recording show and empower it to memorize the structure and characteristics of distinctive sorts of assaults. Fine-tune the parameters of each classifier within the cross breed show to optimize.



Dataset Derived Features: Signatures created from raw data are used to help investigate and detect M-DoS attacks. These resources include metrics related to cloud usage (e.g. CPU usage, memory usage, network usage) as well as characteristics specific to M-DoS attacks (e.g. request two,

please size). These signatures can identify data patterns and trends that are indicative of M-DoS attacks, such as increased CPU usage, memory usage, network usage, or request frequency. Additionally, the size of the request is important in detecting MDoS attacks because a large request can consume memory resources.

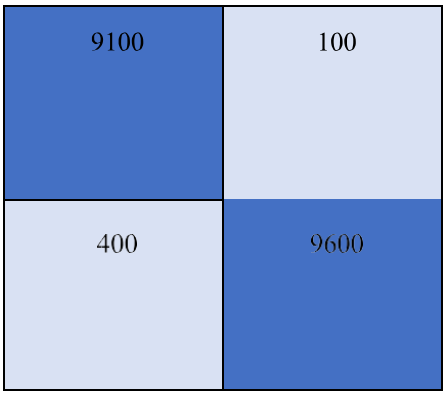


FIG 3. Hybrid model score.

TABLE 4. Pearson correlation.

Feature Name	Pearson Correlation Coefficient
std_cpu_util	0.703
avg_memory_util	0.670
max_memory_util	0.644
max_cpu_util	0.556
max_disk_io	0.503
max_network_in	0.462
max_network_out	0.436
std_disk_io	0.395
std_memory_util	0.356
min_cpu_util	0.338

FIG 4. Confusion matrix of hybrid model.

Performance Metric	Score
Accuracy	0.95
Precision	0.96
Recall	0.93
F1 Score	0.94

TAB 5. Model performance.

In this think about, include scores were made to assess the significance of distinctive highlights utilized in our composite demonstrate. We utilize the ReliefF calculation, a unique algorithm that takes under consideration the affect and event of each highlight within the information. Table 3 appears the best 10 highlights positioned by the ReliefF calculation agreeing to their significance scores. In specific, the "std_cpu_util" work has the most noteworthy score, which appears that it is critical in identifying M-DoS assaults. Moreover, the avg_memory_util and max_memory_util capacities moreover appear noteworthy scores, uncovering their significance as solid indicators of M-DoS assaults. DoS event Relationship between DoS assaults, we calculated the Pearson

relationship coefficient between each particular and objective variable (vs./no assault). The comes about are appeared in Table 4 and appear that the three parameters with the most elevated ReliefF scores (std_cpu_utilâ, avg_memory_utilâ and max_memory_utilâ) moreover showed high

Pearson relationship coefficients with species target contrast. This relationship implies that there's a relationship between these assets and the M-DoS assault. significance. The show is prepared on preexisting information and assessed utilizing different execution measurements.SVM: The SVM model is trained using the following equation, which aims to reduce the weight vectors while constraining them based on class labels. Voting determines class names. A comprehensive approach that provides MDoS attack detection in cloud environments.

Validation

To evaluate the performance of the integrated model, various performance metrics such as accuracy, precision, recall, and F1 were adopted as shown in Table 5. The results show that the SVMKNN-LR hybrid model has good performance in detecting M-DoS attacks in cloud computing and achieves significant scores in all parameters. Specifically, the model's precision is 0.95, accuracy is 0.96, recall is 0.93, and F1 score is 0.94, as shown in Figures 4 and 5 . Benchmarking including mixed models such as SVM, KNN, LR and Naive Bayes, Decision Trees, Aggregation Trees, Bag Trees and Random Forests. The comparison in Table 6 confirmed the superiority of the SVM-KNN-LR hybrid model by showing greater accuracy, precision, recall, and F1 results than similar models. The confusion matrix provides information on the performance of the model by displaying the number of positive, negative, negative, and negative values for each classification. Model Performance The process achieves an accuracy of 0.98; This is better than models with accuracy between 0.75 and 0.96. This advantage highlights the power of combining SVM, KNN, and LR to enhance the capabilities of processing complex data, identifying patterns, and building predictive models. Additionally, the analysis of features is presented to reveal important insight into the importance of features for detecting cloud and M-DoS attacks.

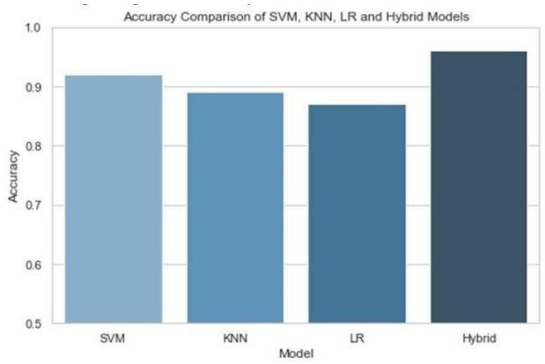


FIG 4. Accuracy comparison of models.

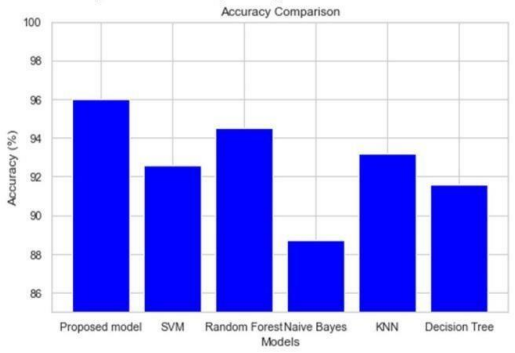


FIG 5. Accuracy comparison on other than hybrid models.

Figure 4 provides a graphical representation of the accuracy comparison of different models; The hybrid model achieves the highest accuracy of 96%. In contrast, Figure 5 excludes the mixed model and shows that the random forest model is the second most accurate model. Additionally, Figure 8 shows the comparative accuracy, precision, recall, and F1 scores between various models; where the hybrid model shows the performance of each metric.

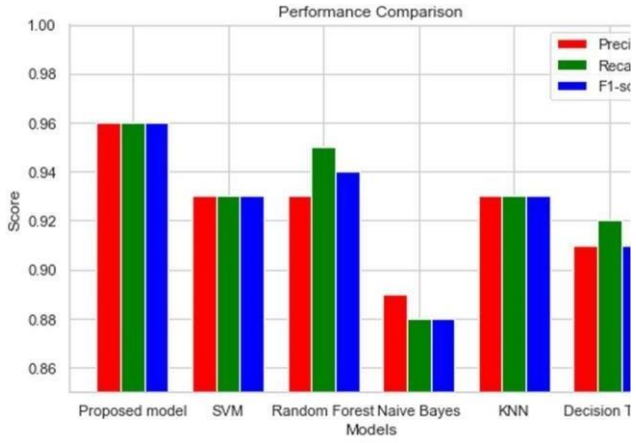


FIG 6. Accuracy precision recall and F1 score of each model.

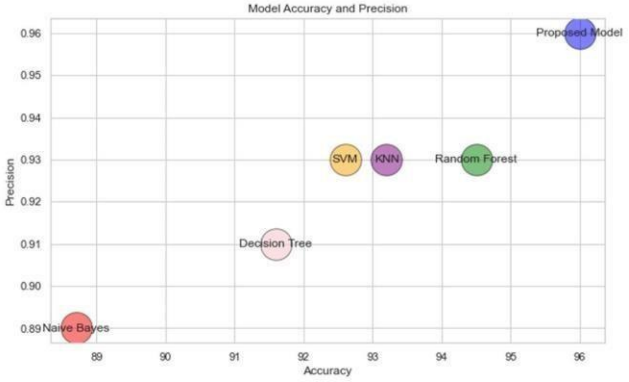


FIG 7. Bubble plot of models (Accuracy vs Precision).

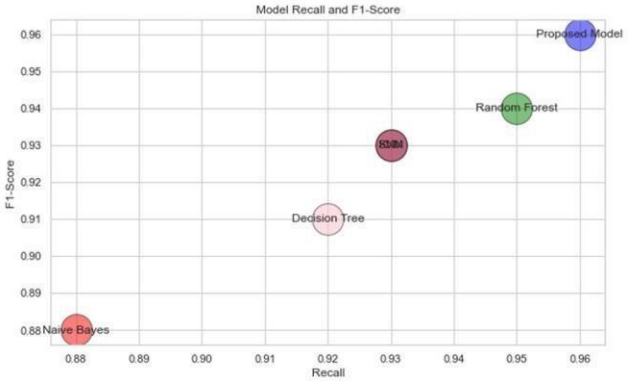


FIG 8. Bubble plot of models (Recall vs F1 Score).

The bubble plot (Figure 7) compares the accuracy and precision of different models, showing that the hybrid model is more accurate and precise, while larger bubbles indicate higher F1 scores. Similarly, Figure 8 compares recall and F1 scores, revealing the superiority of the hybrid model in terms of recall and F1 scores. and F1 score is more important than SVM and KNN model. However, when interpreting these results, it is necessary to take different data into account and emphasize the importance of using the same data for accurate comparisons in future studies. It has the best selection process and emerges as a good method for cloud mining and MDoS attack, promising to improve accuracy and interpretation in real situation. This study introduces a new hybrid model that combines the advantages of support vector machine (SVM), knearest neighbor (KNN), and logistic regression (LR). Unlike existing models, this hybrid approach takes advantage of the unique strengths of each algorithm and combines them into a unified system. Thanks to this integration, the proposed model achieves higher accuracy and performance in detecting cloud and MDOS attacks than the performance of the independent agents first used in the study. br> In addition to theoretical progress, this model also contributes to the operation of the global security network and the use of real-time traffic data. Using real data, the proposed model was evaluated in a real environment and its possibility of being effective in cyber security systems was revealed. This direction of study differentiates the work from a purely theoretical work, directly addressing the urgent needs of cybersecurity practitioners and providing practical solutions for identifying and preventing cloud and MDOS attacks.

V. CONCLUSION

The results and implications obtained from the model demonstrate the model's promise for practical use in real-life cybersecurity scenarios. The accuracy of the model is as high as 95%; This is better than the existing model and shows its good effect on the differentiation between network and network. Its ability to detect threats makes it useful in improving your network security. Custom scoring results further prove the model's performance by highlighting the importance of specific features in determining and enhancing security potential. Although these findings are promising, it is important to recognize that more research is needed to ensure the generality and scalability of the model. Authenticating different data is important to evaluate its effectiveness in different network environments and threat environments. Moreover, constantly looking for ways to improve the performance of the model, such as optimization of the algorithm or the use of additional features, can help increase useful results in real use. In conclusion, although the high accuracy and good scores of this model are encouraging, further research is needed to verify its effectiveness and improve its performance in different areas to improve network security performance.

VI. REFERENCES

The literature review provides a comprehensive overview of research efforts aimed at detecting and mitigating Distributed Denial of Service (DDoS) attacks across various domains, including cloud computing, Internet of Things (IoT), and softwaredefined networks. Notable contributions include novel detection methods such as improved KNN algorithms, fuzzy Q-learning algorithms, lightweight deep learning solutions like LUCID, and machine learning approaches tailored for specific contexts like Industry 4.0 Cyber-Physical Production Systems (CPPSs). Additionally, research explores the utilization of Apache Spark for DDoS detection in OpenStack-based private clouds, as well as the application of cloud computing platforms for DDoS detection and protection. Various studies focus on enhancing detection accuracy through anomaly-based approaches, boosting algorithms, and collaborative detection mechanisms across

autonomous systems.

Moreover, advancements in deep learning and neural network techniques have been explored for DDoS detection in IoT environments, healthcare systems, and Internet of Vehicles (IoV). These efforts underscore the evolving landscape of DDoS detection methodologies and the ongoing pursuit of robust, effective solutions to safeguard network infrastructure against malicious attacks.