International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Machine Learning Algorithms for Distributed Denial of Service (DDoS) Detection in the Banking Sector using IoT-Based Monitoring Techniques

Abhi Agola[1], Yash Desai[2], Arju Desai[3], Rajiv Khurana[4], Shubham Kumar[5], Vivek Dave[6]

Submitted: 01/11/2024 **Revised:** 20/12/2024 **Accepted:** 29/12/2024

Abstract: Large-scale cyberattacks are becoming more and more likely to target banks. Because banks are interconnected, a cyberattack on one might put the solvency of a financial establishment at risk. Cybercrime has increased since more people use mobile banking and the Internet. Fraudulent activities such as identity theft, ATM robberies, and credit card scams are examples of cybercrime. The substantial financial the data's value held by the banking industry makes it particularly vulnerable. The potential attack surface has increased with the growth of banks' digital footprints. Cyberattacks have the potential to result in confidential information leaks, power disruptions, and malfunctioning military equipment. They might lead to the theft of priceless private information. They can paralyze systems or interfere with computer and phone networks, making data unavailable. The banking sector is especially vulnerable because of the substantial financial value of the information it contains. Hackers can make money in various ways using the financial data and banking credentials they have taken.A distributed denial-of-service attack (DDoS) is a type of online fraud that can affect the speed at which websites load, especially those run by other financial organizations and banks.DDoS attacks happen when many systems overwhelm a targeted system's resources or bandwidth.The machine learning (ML) models address the aforementioned informational challenges. The amount of digital footprints that banks have increased increases the attack surface available to hackers. This research uses the Caida dataset to identify DDOS attacks against financial establishments. This work proposes a mathematical model for DDoS attacks. ML algorithms like Naive Bayes (NB) and Logistic Regression (LR) are employed to identify attacks and typical situations. This dataset tests and trains ML algorithms; the results validate the learned algorithms. The Weka data mining platform is used in this investigation, and the outcomes are examined and contrasted. The current study is contrasted with other ML methods utilized concerning DDoS attacks.

Keywords: *DDoS attack, DoS attack, Naive Bayes, Logistic Regression, Machine Learning model, Banking Sector, Cyber-attacks, Cybercrime, Mathematical models*

1. Introduction

In ML, the difficulty of detecting a DDoS attack is a classification problem. Identifying DDoS assaults poses a significant challenge in cloud computing due to the computational complexity involved.At their core, DoS attacks are deliberate attempts by a single source of attackers to implicitly prevent the target stakeholder from using a program. To do this, attackers typically divide the available network bandwidth, stopping system functions and refusing authorized users access.DDoS attacks differ from DoS attacks because attackers use several sources to launch them. Generally speaking, DDoS attacks can be classified according to the OSI model layer that they target. Application, presentation, transport, and network layers are where they are most prevalent **[1].**With the rapid expansion of Internet technology, hundreds of thousands of gadgets can now operate online. The Internet is becoming widely used in various fields; it has grown and is open to multiple threats. The most common types of these assaults are DDoS and DoS.DoS attacks can be launched in a variety of ways. DDoS and DoS attacks aim to exhaust network resources as their primary goal and to prevent programs from providing services to users. DDoS assaults happen when zombie devices bombard the hosting server with unnecessary traffic **[2].**DoS attacks have historically been mainly used to interfere with networked computing systems. These attacks are essentially directed towards a server system maliciously from a single

[1,2,3,4,5]*Parul Institute of Engineering And Technology (MCA), Parul University, Vadodara, Gujarat*
[6]*Assistance Professor, , Parul Institute of Engineering And Technology (MCA), Parul University, Vadodara, Gujarat*

machine. A PING Flood attack is a simple DoS attack in which the computer delivers the target server ICMP requests. An advanced kind of DoS attack is called a Ping of Death attack. DDoS attacks are preceded by DoS attacks, or more precisely, DDoS attacks are the post cursor to DoS attacks. DDoS assaults are those that are launched in geographically dispersed locations. A DDoS attack is a form of intentional attack commonly encountered in distributed computer environments to reduce a server's or website regular performance.An attacker employs several systems within a network to accomplish this. Using these systems, the attacker inundates the target server or website by submitting several queries to the target system.Because they occur in dispersed environments, these attacks are often called distributed DoS attacks.The issue of preventing, detecting, and mitigating DDoS attacks has gained much attention concerning cloud computing environments. Researchers have given the problem of DDoS attack detection the highest priority out of these three concerns.Scholars worldwide have been consistently engaged in formulating diverse techniques and strategies to tackle the issue of DDoS assault detection. Unfortunately, despite several contributions addressing strategy and tactics to prevent DDoS assaults, the adoption of existing strategies was unable to fend off DDoS attacks that negatively impacted cloud systems. In actuality, attacks' frequency and size significantly rise over time. Since cooperation cannot be enforced globally, one of the most frequent causes of a distributed internet network is the need for more consensus among different endpoints.The economic variables may be the second cause, as they complicate the enforcement of global collaboration. The third reason is single-point deployment cannot be best ensured or enforced to defend against the attacks.Data from Amazon Web Services indicates that February 2020 has seen the most significant DDoS attack.This attack is noticed to have 2.3 Tbps of peak inbound traffic.Attackers employed compromised CLDAP webservers, a protocol that handles user directories and replaces LDAP, as their weapon of choice.The February 2020 1.3 Tbps DDoS attack was the second-biggest, with 126.9 million packets sent per second towards GitHub.As a result, it is becoming increasingly important to thoroughly examine, pinpoint, and determine the causes of the methods' shortcomings as reported in the investigation literature. Both the strength and frequency of DDoS and DoS attacks are rising. Every day, on average, 28.7k attacks are launched. In the first half of 2019, the frequency of DDoS attacks increased by 200%, while their volume increased by 73% in 2018, according to Neustar's Cyber Threats and Trends Survey. According to predictions, there will be twice as many DDoS assaults by the end of 2023 as in 2018, with a potential total of 15.4 million attacks.According to Neustar's Cyber Threats and Trends Report 2020, attacks increased by 151% in June 2020 over the same month in 2019. Furthermore, the highest assault intensity has increased by 81%, and the most significant attack size has increased by 192%.Additionally, the assault volume climbed to 12 Gbps in June 2020 from 11 Gbps in the same month in 2019. Consequently, there is a greater need to create a method for successfully and effectively detecting DDoS attacks **[3, 4].** The DDoS attacks DNS flood, HTTP, UDP, ICMP, TCP, and SYN are highly recognized **[5].** Figure 1 displays DDoS attack types along with their subtypes.

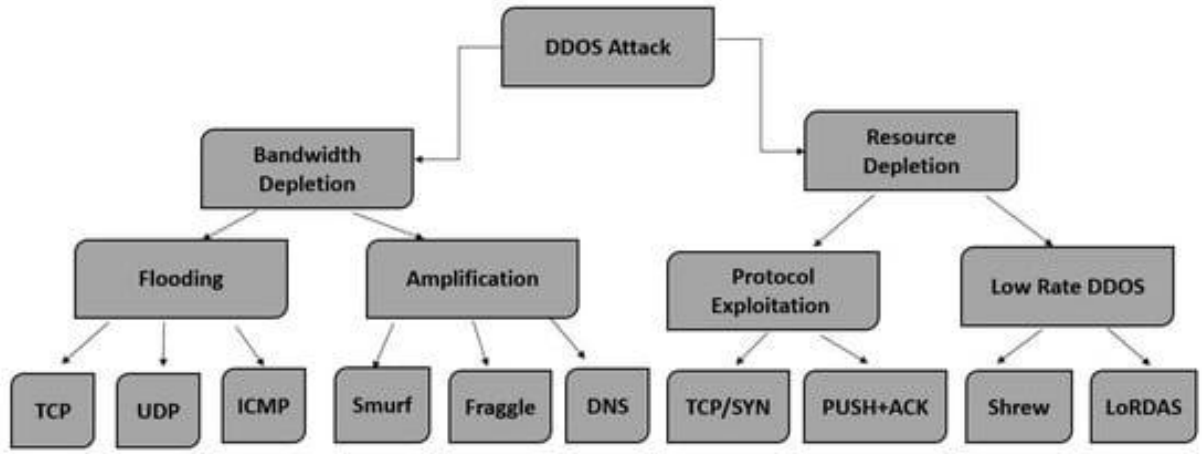

Figure 1 DDoS attack types along with their subtypes.

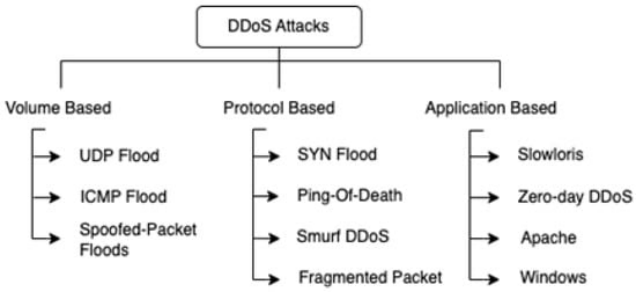

Figure 2An overview of the various methods by which DDoS attacks can be executed.

DDoS attacks are one of the most severe threats to IoT network security. The attacker leverages the target's resources by creating considerable network traffic over multiple infected nodes, which overwhelms the victim. Ultimately, this leads to service disruptions, infrastructure degradation, and authorized users being unable to access connected services.Using a reflection amplification attack approach, attackers can increase the volume of malicious communication they produce while also hiding the attack traffic's sources.The attacker sends packets to several locations using the reflection technique, using the IP address of the target as the packet's originating address.The attacker, on the other hand, employs the amplification strategy to bombard the target's system with packets.**Figure 2** provides an overview of the various methods by which DDoS attacks can be executed.DDoS attacks have affected several large IT organizations in recent years; In February 2020, AWS was the target of one of the most severe attacks. Massive traffic streaming at roughly 2.3 terabits per second (Tbps) was used to mount the attack. In a similar vein, the DDoS attack in 2018 also attacked GitHub.Several areas of modern life, including education, transportation, finance **[6],** healthcare, entertainment, personal usage, e-commerce, communication, trade, administration, **[7, 8, 9, 10],** the environment **[11],** and many more **[12, 13],** depend heavily on the internet.Human life has been made more accessible by this revolutionary shift in communication and technology. As technology progresses, several hazards connected to security also surface and increase. This is also proper concerning internet security, as there has been a noticeable rise in data loss, resource theft, confidentiality violations, online fraud, social harassment, etc**. [14, 15, 16, 17].**Access to data is one of the primary problems with network security.One of the most frequent attacks that compromise a network's availability is DDoS. It does this by taxing the system's services with frequent requests for the desired resources.

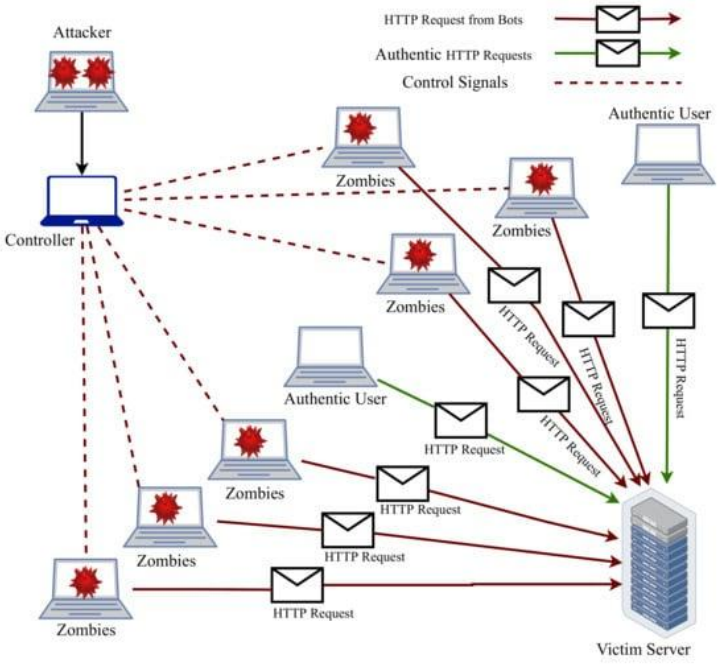

Figure 3A DDoS assault schematic.

As seen in **Figure 3**, a DDoS assault consists of requests from several systems to one target.DDoS attacks allow malicious users to manipulate the availability of services and systems for authorized users. DDoS attacks are on the rise right now, endangering network security. DDoS assaults have historically used botnets, which are collections of infected systems.This attack's primary goal is to destroy the server's memory, bandwidth, processor, and other resources to stop services for authorized users. A thorough analysis of current DDoS attacks may be found in **[18],** and several mitigation strategies are covered in **[19, 20, 21].**DoS attacks are categorized based on several factors. DoS attacks' application and transport layers additionally divide an attack based on network protocol.

1.1 ML detection models for DDoS Attacks in IoT Networks

The idea behind the IoT is to give physical items and things the ability to generate, process, and exchange data. Increasing efficiency and giving us total control over our lives is the fundamental purpose of the IoT. Even while objects are intelligent enough to function without human assistance, their owners have authority over them.Sensors are used by IoT devices to gather vast volumes of data and minimize the need for human data entry. However, it is commonly recognized that IoT devices have limited processing power and storage capacity, highlighting the condition of the cloud. The term "Cloud of Things" (CoT) refers to the nexus where cloud computing and IoT devices come together to help overcome the abovementioned constraints. The cloud provides the services and infrastructure required to power IoT devices. In 2021, there will be 12.3 billion active endpoints worldwide, according to IoT data, translating to a 9% increase in connected IoT devices. By 2025, there will be over 27 billion IoT connections. Specific IoT devices have time-sensitive applications. Therefore, the gathered data must be processed and examined right away.The performance of cloud computing can be significantly impacted by network latency or the delay in data transmission over a network, which can ultimately compromise the system's overall efficacy.Fog computing may act as a mediator between endpoints and distant cloud servers. It does local processing and low-latency computing in real-time. Thus, fog is an intelligent gateway that offloads cloud processing, allowing for more effective computing, data processing, and analysis **[22].** Figure 4 shows the architecture of Fog Computing. CISCO promotes fog computing as an effective method of extending cloud computing and related services to the network's edge. Many organizations, scholars, and network specialists have defined and described fog computing from various angles.

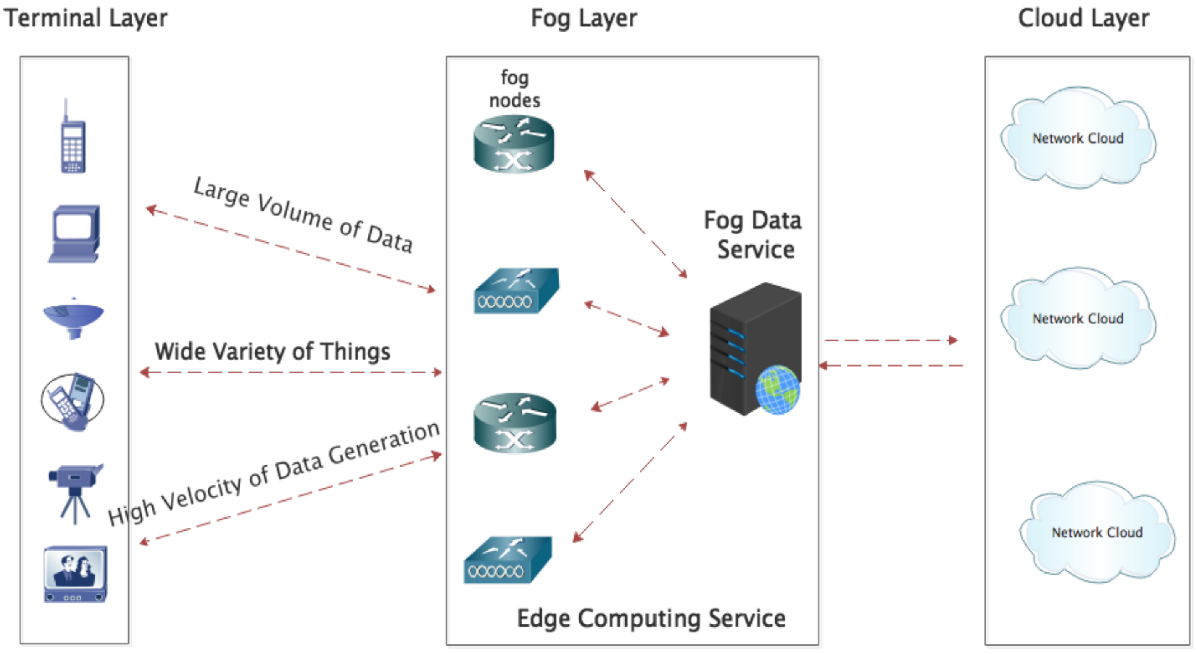

Figure 4Architectureof Fog Computing

1.2 DDoS attack and Banking Sector

Chayomchai et al. **[23]** are investigating the effects of cybercrime on financial institutions and the measures implemented to mitigate those impacts. The most recent victims were banks. Massive cyber-attacks regularly steal sensitive and essential data and cause significant financial losses to target Indian institutions.According to this study's conclusions, a customized cyber-security plan should be created to safeguard a company's most susceptible areas from cyberattacks. The study includes secondary data analysis from official publications, websites, scholarly investigations, and case studies of earlier cyber risks and crimes resulting in substantial monetary losses. This study aims to provide banks, financial establishments, and the general populace with an adequate understanding of the cyber control. Latent Dirichlet Allocation (LDA) combined with symmetric Kullback-Leibler divergence on tweets may be used to construct weakly supervised models that calculate the effect of DoS attacks without data annotations. The module has a limit that is only partially monitored. Within the pre-specified detection window, fewer non-attack Twitter events are likely to be misidentified as DoS attacks, As a result, this issue is likely to become negligibly intense.Non-attack tweets can be eliminated from the dataset as an alternative by employing an additional classification layer trained on manually annotated DoS attack tweets. In the same sector, precise and generalizable models can be produced using weakly-supervised learning algorithms **[24].**Innovative technology can be used to identify abnormal behavior in online bank customers, as noted by Alimolaei et al. **[25].**System designers employed the fuzzy theory to account for the fact that uncertainty sometimes accompanies user actions. The performance of the fuzzy expert system was examined using a receiver operating characteristic curve, and the results suggest that it is 94% accurate. The Internet Banking safety and quality of service may be enhanced by employing this expert system. The numerous online risks associated with banking. It also offers a method for cyber-banking security that emphasizes safeguarding the application's boundaries. There are two distinct methods for protecting the infrastructure of a system: application security and peripheral security **[26, 27].**

2. Review of Literature

2.1 DDoS attacks against networks based on the Internet of Things

A review of the numerous studies conducted on employing ML to identify DDoS attacks against networks based on the Internet of Things is shown in **Table 1**. After the research was examined from three perspectives—the dataset, the ML level, and the fog layer, certain shortcomings in the literature were discovered.

Table 1 Employing ML to detect DDoS attacks against networks based on the Internet of Things-Review

Dataset	Number of features	DL/ML models	Model's accuracy	Rate of performance	Year	Reference
Generated	IoT network behavior is represented by 26 aspects that rely on network flow data.	LR,NB,NN, DT, RF, SVM	RF	F-Score (97.8%) recall (98.9%), Precision (96.7%), Accuracy (99.2%)	2022	**[28]**
CIC-IDS2017	80	QDA, Naive Bayes, MLP, Adaboost, ID3,RF, KNN	ID3, RF, KNN	-	2017	**[29]**
Generated	Three characteristics are stateless and three are stateful.	NN, DT, LSVM, KNN, RF	NN, DT, LSVM, KNN, RF	F1-Score , recall, precision, Accuracy, Greater than (99.0 %.)	2018	**[30]**

Modified CICIDS2017	15 of the 85 features were chosen	RF, Bayes, SVM, MLP, IDS, NSGA-II-aJG	SVM	Accuracy (94.50%)	2020	**[31]**
Generated	27	Naïve Bayes, J48, MLP, RF	DT, J48	Accuracy (98.64%)	2020	**[32]**
Generated	40 of the 115 were chosen	RF, DT, NN, LSVM	DT and RF together	Error MAE (RF = 0.37%), DT = 0.31) F1-Score (99.7%), recall (99.7%), precision (99.7%), FPR (0.3%), TPR (99.7%).	2020	**[33]**
NSL-KDD	-	RF	RF	Accuracy (99.76%)	2021	**[34[**
BoT-IoT	The Chi-Square was used to determine the 8 eight features.	ANN, MLP, Bayes, Naïve, Gaussian, KNN	KNN	AUC (92.2%) ROC (92.2%) Accuracy (92.1%), on extremely skewed real-time data	2021	**[35[**
CICDDoS2019	Top 10 features	R, KNN, XGBoost, AdaBoost, , SVM, Bayes, Naive	XGBoost, AdaBoost	F1-Score (100%) Accuracy (100%),	2021	**[36[**
CCD-INID-V1	83	RF XGBoost,	RF and XGBoost together	-	2021	**[37[**
CICDDoS2019	Among the 79 features, the best features were chosen using an ANOVA, a chi-squared test, and an extra tree.	XGBoost, KNN, DT, RF	ANOVA and XGBoost together Fifteen features	XGBoost + extra tree: accuracy (92.78%), XGBoost + chi-squared: accuracy (92.67%), F1-Score (99%, recall (99%), precision (99%), and accuracy (98.347%) ANOVA test	2021	**[38[**
BoT-IoT	Top 10 features	LSTM RNN, MLP, KNN, RF, DT	RF, KNN	99.81% RF Accuracy while using the looking-back method, KNN Accuracy (99.93) in the	2022	**[39[**

				absence of the looking-back method;		
KDD Cup99	60	ANN Only	-	-	2022	**[40[**
UNSW NB15., BoTIoT, UNSW2018, NBaIoT2018, DoHBrw 2020, CICDDoS2019,, CSE-CIC-IDS2018, CICIDS 2017,	2	VMFCVD (DFDM, FDM, HAM, modes) RF, KNN, GB, Bagging, AdaBoost,	VMFCVD (HAM mode)	F1-Score (99.99%), precision (99.99%), Average accuracy (99%),	2022	**[41[**
BoT-IoT	There were three distinct feature sets with 35 variables, ranging in number from 15 to 18.	RF DT, SVM are ML MLP, GRU, LSTM, RNN, are DL	DT (robust) and RF outperforms the DL models	F1-Score(100%), recall (100%), precision (100%), accuracy (100%), Average accuracy (99%)	2022	**[42[**
Kaggle banking dataset	Using the homogeneity measure (k-means clustering) to choose key features	RF, KNN, SVM	SVM	F1-Score (98.5%), recall (98.32%), precision (99.07%), Accuracy (99.8%)	2022	**[43[**
UNWS-NB15	-	XGBoost, RF	XGBoost	F1-Score (90%) Recall (90%), Precision (90%), Average accuracy (90%)	2022	**[44[**
CICDDoS2019	Out of 88 features, the "Extra Trees Classifier" determined the top 15 features.	ANN, RF, DT, KNN	ANN	F1-Score (99.97%), recall (100%), precision (99.95%), Accuracy (99.95%)	2022	**[45]**

Several methods for detecting and preventing network attacks have been introduced recently. Hybrid, anomaly-based, and Signature-based structures are the three types of intrusion detection systems (IDS) **[46].**The first kind compares the event with an internal database that has signatures to identify irregularities. The second technique makes use of variations between the present

condition and the regular state of the database to identify assaults. In all cases, the discovery of a corresponding likeness or the detection of a variation may raise an alarm. Although signature-based intrusion detection systems are renowned for having a low false alarm rate, gathering and storing potential attack variations is extremely difficult **[47].** Writing signatures for each possible attack variant is a task, though. Although additional evaluation resources are needed, anomaly-based detection systems can also discover other sorts of attacks. Hybrid techniques combine the advantages of both methods**[48, 49].**In recent studies on extensive data, wireless networks, cloud computing, etc., flooding attacks have received much attention **[50, 51, 52].**Numerous categorization strategies for DDoS attacks have been put forth recently.Network-level attacks and application-level DDoS flooding are the two types into which DDoS attacks can be divided at the protocol level **[53].** Early identification and impact reduction of DDoS assaults are two main challenges.However, it requires a few extra properties absent from the existing methods **[54].** In **[55],** the HTTP-based method for data sampling-based HTTP flooding attack detection is provided. The CUMSUM algorithm is the foundation of the study's traffic classification as harmful or benign.Traffic analysis uses two metrics: the total number of packets with zero sizes and the total number of application layer requests sent. According to the results, using a 20% sample rate, the method yields a detection rate of 80% to 86%. The D-FACE algorithm is used in **[56]** to describe a DDoS assault detection system. This technique detects DDoS attacks using generalized information distance (GID) andgeneralized entropy (GE) matrices. The industrial applicability of the proposed technology is limited due to the substantial involvement required from internet service providers (ISPs).Sky-Shield technology was created to protect against DDoS attacks at the application layer. **[57].** It considers two hash drawings to locate divergence to detect anomalies in traffic flow. User filtering, whitelisting, and Blacklisting are removed as defensive measures during the mitigation phase. Customized datasets are used to assess the outcomes. Sky-Shield is susceptible to network-level flooding andtransport- and attacks because its primary focus is identifying at the application layer flooding attacks, particularly concerning the HTTP protocol. Another possible approach for DDoS flooding attack detection entails employing a semi-supervised-based method, as described in [58], to detect and combat DDoS flooding attacks.Distinct clustering techniques are applied, and voting controls the final label. The evaluation procedure makes use of the CICIDS 2017 data set.**Table 2** summarizes a list of related works. Significant computational costs and great accuracy outcomes are cited in scholarly works from investigations that use sophisticated deep learning (DL) models. On the other hand, simple solutions have a cheap computing expense, but they perform poorly in terms of accuracy of attack detection. Our goal is to go past this constraint by creating a noteworthy method for its accuracy and computing expenditure.

Table 2Asummary of related works.

Objectives	Models	Dataset	Limitations	Year	References
IoT devices in the banking sector DDoS attack identification.	An open-source dataset about DDoS attacks	RF SVM KNN	The precision/accuracy of their suggested strategy has to be increased.	2022	**[59]**
DDoS attack on the application and transport layers of Internet of Things devices	Bot-IoT	LSTM,GRU,MLP DT,SVM,RF	The distribution of targets in binary classification needs to be more balanced in this investigation.	2022	**[60]**
Ensemble learning is used in SDN networks for	Utilise the RYU API to gather their dataset for	Ensemble SVM-RF, RF, SVM	Using an ensemble learning strategy means paying more for	2021	**[61]**

DDoS attack detection.	DDoS and SDN networks.		computing. The computational cost of the SVC model in the ensemble is substantial.		
ML and statistical techniques are used for DDoS detection in SDN.	LR, NB, J48, REPTree	ISOT datasets, CTU-13, NB-ISCX	Because these studies used simplistic models, they were economical in computing power but at the expense of accuracy.	2021	**[62]**
DDoS attack identification in real-time using big data in real-time.	MLP, RF	Public platform with Application-Layer DDoS Dataset accessible -Kaggle	They focus on accuracy and efficiency, but we needed more data to determine the approach's importance because they were limited to two models	2021	**[63]**
identification of various DDoS attacks, including ICMP, TCP, and UDP floods, among others	NB, RF, KNN	Wireshark	The suggested method used straightforward models with cheaper computational costs but worse accuracy than other methods	2020	**[64]**
Detection of malicious communications by the use of ensemble learning.	ETC, GBM, RF	IoTID20, UNSW-NB15	They used a lot of computing power to build a stack of models.	2021	**[65]**
Identification of DDoS attacks using SDN-based architecture.	RF KNN, MLP, LSTM,GRU	DoS2019 CICD115 CICDoS2017	Since the application layer's attack detection rate is 95%, the results of the suggested system for the transport layer and application are different. Second, they made use of computationally expensive, intricate GRU models.	2021	**[66]**

2.2 DDoS attacks and Banking sector

With a revolutionary technique created by Salem et al. **[67],**it is now feasible to check e-banking transactions for potential fraud. The objective is to identify fraud by combining a model with scoring parameters for past offline and online transactions in real-time, which is the objective of detecting fraud.Data processing on a large scale, an approach to analyzing massive transaction logs, is shown, along with an architecture based on MPP Gbase, Spark, and Kafka.The author's experimental results over a sizeable electronic banking transaction dataset show the proposed technique's effectiveness. Future study by the author should fill in these gaps and move beyond these obstacles.Cybercrime datasets are analyzed [68], and issues that are easily accessible are noted using the J48 Prediction Tree, Influenced Association Classifier, and K-Means accessible issues **[69].**

Influenced Association Classification makes use of the K-Means clustering technique. The J48 method allows K-means classifiers to mine the record and forecast cybercrime by employing K-means selection to determine the first centroids.With the help of combining data from the J48 Prediction Tree, Influenced Association Classifier, and K-Means, bank cybercrime may be predicted more precisely and effectively. Law enforcement officials belonging to the author must be adequately prepared to tackle and avert cybercrime.Authors of **[70, 71, 72]** discussed the difficulties that several banks and card-based businesses experienced. A comprehensive problem investigation is required to provide a workable and efficient solution. Information exchange can assist in protecting a bank against cyberattacks.Steer clear of accepting too many queries at once from the user session or same source **[73, 74].** Most automated attack sources make requests for web pages faster than human users. It is vital to safeguard the network and its applications against DDoS attacks.Network methods such as packet fragmentation, spoofing, or breaking TCP handshakes are often used in DDoS assaults. Application-level attacks aim to exhaust the server's resources.One can evade anti-malware attempts using known program attack signatures and identifying unusual user behavior. It is possible to locate DDoS assaults by searching for recognizable patterns or signatures. IHTTP requests that don't adhere to the protocol's guidelines are expected in DDoS attacks. One widely acknowledged aspect of the Slowloris attack is HTTP header repetition. A DDoS client can attempt to visit sites that are not present. Attacks could also cause a sluggish web server or delayed reaction times.The authors of **[75,76]** have discovered that computer resource security and bandwidth availability are still issues even though many protection mechanisms exist. The DDoS issue grew more severe due to increased legitimate traffic that resembled attack activity. This work demonstrates how autonomous system routers equipped with T-CAD, a distributed attack detection system, can identify and mitigate DDoS attacks. For instance, T-CAD uses the normalized router entropy to differentiating DDoS attacks, flash events, and regular traffic. Thus far, tests on OMNeT++ and INET have demonstrated the functionality of the proposed attack detection system. In simulated testing, the T-CAD DDoS defense system has outperformed many existing entropy-based and thresholds DDoS detection methods. The different models of DDoS attacks, together with a chronology of defense strategies and advancements to stop them, are all examined in the research presented by **[77,78].** We have developed a novel DDoS assault detection system using MapReduce programming architecture.The Internet banking platform states that different processes are used for customer authentication. While some banks employ PINs and passwords, others utilize TANs and TAN lists (sometimes called scratch lists) for transaction authorization and verification. More sophisticated methods like challenge-response systems and one-time passwords can also authenticate users.The author believes significant banks still need public-key certificates to authenticate customers successfully.The TLS/SSL protocol's cryptographic power is frequently cited in defense of the security of online banking. The TLS/SSL protocol's security has vulnerabilities and few documented theoretical weaknesses.This research makes use of the Dolev-Yao threat model.An attacker can hijack the communication channel between a server and a client, but the channel's endpoints are consistently secured. It is inaccurate to portray the actual ways in which a hacker could damage a client.Mehmood et al**. [79]** use a Hidden Markov Model (HMM) to avoid fraud in online banking. As a result, each enrolled consumer receives a one-time password by text message from the bank's system, ensuring that only valid transactions are rejected. To avert catastrophic losses, banks are implementing fraud detection and prevention technology. Financial institutions worldwide use state-of-the-art fraud technologies to identify and halt fraudulent Internet banking activities. Their inability to effectively identify and track authorized users is the problem. The author suggests utilizing a Hidden Markov Model as a remedy.To illustrate the various attack techniques cybercriminals employ against specific Indian banks. Research **[80]** has tried to show how Indian banks in the private and public sectors are connected to spoofing, brute force attacks, cross-site scripting, and buffer overflow. System monitoring and intrusion detection are also related to cyberattacks such as online identification thievery **[81],** malicious code, hacking, ATM/credit card fraud,hacking, and DOS attacks **[82, 83].**DDoS mitigation based on blockchain is a feasible and promising strategy. The inherent

qualities of blockchain, including its decentralization, immutability, verifiability, anonymity, and lack of external and internal trust, may neutralize this grave cyber threat.Considering how DDoS mitigation utilizing blockchain technology works out in several firms, we believe there is no need for citations in such comments. This study will examine several solutions in detail, emphasizing their benefits, limitations, and downsides. The growth of DDoS mitigation research and techniques will benefit from a single platform for learning about contemporary tactics.Collaborative DDoS attack detection approaches that consider detection performance in different time zones are used to recognize DDoS attacks on several networks more accurately. Every network's detection and "false positive" rates are weighted according to its time zone to determine the overall assessment of individual assaults on every network. Suggests utilizing weighted detection data to ascertain whether a DDoS attack has occurred. The suggested approach reduced false positives by 35% while maintaining a significantly increased detection rate. Although this work aims to identify and characterize those characteristics, the optimal prerequisites for a protective solution remain to be found and documented **[84, 85].**This work aims to thoroughly define and pinpoint the ideal parameters for a defensive architecture against these kinds of attacks. It has looked at all types of HTTP-based DoS and DDoS attacks. Diverse DDoS detection techniques have been developed in the past by several researchers using divergence measures and information theory entropy.Research suggests utilizing a novel "LeCam divergence metric" based on flow similarity across network traffic flows to identify distinct DDoS attacks. The suggested methodologies can be applied successfully, as demonstrated by experiments conducted on MIT Lincoln and CAIDA datasets. The LeCam Divergence metric performs better than the conventional Kullbeck-Leibler Pearson Divergence measures and Bhattacharyya.DDoS attacks can be classified as either DDoS attack traffic or harmless traffic thanks to a novel architecture that combines a well-posed sparse Auto Encoder (AE) for feature learning with a Deep Neural Network (DNN) for classification **[86].**By modifying the AE and DNN settings in a way intended for this purpose, attack detection is more straightforward. The author of this study describes how to eliminate disappearing or gradient inflating, decrease reconstruction error, and create a network that is smaller and has fewer nodes to prevent overfitting **[87].** Performance metrics like recall, F1-Score, detection accuracy, and precision were utilized to assess how well the suggested method performed compared to ten established best practices. To confirm the findings, a number of tests have been run on the CICIDS2017 and NSL-KDD standard datasets. The suggested approach performs better than the current one.DDoS attacks have been reducing network availability for decades, and there is currently no working security solution to stop them. The development of software-defined networking technology has made new defenses against DDoS attacks conceivable. Two approaches have been created to recognize DDoS assaults. Estimating a DDoS attack's power can be achieved in part by locating its source.ML is used to develop the KNN algorithm to locate the DDoS attack. When tested on real-world datasets, when it comes to identifying DDoS attacks, The recommended algorithms by the author surpass those of other scholars. An insider attack is more probable if someone with authorized access to the system subverts the security measures. Early Detection and Isolation Protocol, or EDIP, can be used to stop anti-DDoS attacks. Among the authorized consumers of the system, EDIP locates an insider by forwarding it to an attack proxyA novel algorithm has been devised to enhance the isolation of attacks and minimize disturbance to innocent customers. Proxies can avoid overloading by employing the load-balancing technique. Spectral gene set filtering (SGSF) is a revolutionary technique for filtering gene sets developed by researchers to overcome the issue of extensive gene-setcollections restricting statistical power.

3. Proposed Method

A DDoS is a cyberattack that leverages the power of numerous compromised systems to interfere with network connectivity or service, causing a DoS for users of the targeted resource. This study suggests ML and math methods for DDoS assault detection.The connection between throughput and the inter-arrival time of requests is derived from the presented mathematical model. An additional throughput study was performed to detect DDoS attacks. ML models for identifying DDoS assaults are constructed using LR and NB models.With the aid of a mathematical model, it is possible to

calculate the system's quantitative behaviour.Finding the benefits and drawbacks of a mathematical model is as easy as comparing its quantitative output with facts. Thus, this part proposes a mathematical approach to detect DDoS attacks. The two most important factors in determining assaults are throughput and bandwidth. Throughput measures the quantity of data effectively carried from the source to the destination, while bandwidth indicates the amount of data that can be transported across a communications channel.The likelihood of bandwidth exhaustion is given by Equation 1. which serves as the foundational formula to determine the correlation between the inter-arrival time of requests and throughput. The conclusions of the final derivations, where throughput and inter-arrival time are inversely proportional to one another, are displayed in equations 4, 5, and 6. Equations 8 and 9 are used to compute throughput.

$$P_{BC} = \frac{\left(\frac{\alpha^C}{C!}\right)}{\sum_{i=0}^{c}\left(\frac{\alpha^i}{i!}\right)} and \alpha = \frac{\beta_{AB}+\beta_{LB}}{\beta_{Total}} \ , Cisunusedoropenbandwidth \quad (1)$$

$$\beta_{AB} = \frac{TP_A}{I_{AB}} and \beta_{LB} = \frac{TP_{LB}}{I_{LB}} \quad (2)$$

Assuming that the packet size remains constant for both attack and regular traffic scenarios, i.e.

$$TP_A = TP_{LB} = T_B \quad (3)$$

$$\alpha = \frac{T_B}{\beta_{Total}}\left[\frac{1}{I_{AB}} + \frac{1}{I_{LB}}\right],\ \alpha\ is\ average\ bandwidth \quad (4)$$

$$\alpha = K\ \left[\frac{1}{I_{AB}}\right],\ K = \frac{T_B}{\beta_{Total}}\ K\ is\ conatant\ \frac{1}{I_{LB}}\ ,\ \alpha \propto \frac{1}{I_{AB}} \quad (5)$$

$$P_{BC} \propto \alpha \propto \frac{1}{I_{AB}} and P_{BC} \propto \frac{1}{C} \quad (6)$$

The attacks are identified by measuring the inter-arrival time—the difference between the arrival times of two consecutive data packets—based on the conclusions drawn from Equations 5 and 6.A 10-second sliding window is employed to examine this arrival time. The mean inter-arrival time is computed using the formula in Equation 7.Gaussian distributions are utilized for regular clients, and Poisson distributions are used for attack packets.This study analyzes the throughput and inter-arrival times of the attack and the usual scenario using Caida datasets to provide real-time estimates.Equations 8 and 9 highlight the formula utilized in this procedure.For every 10 s interval, 20090 unique IP addresses are considered.Throughput computation for attack and regular scenarios is displayed in **Table 3.**The throughput threshold is defined as the median value, or 755.97. A throughput beyond the threshold is deemed high and classified as an attack. When the throughput drops below a particular threshold, it is considered low and classified as normal. An acceptable Miss Rate of 0.0025 is found in the mathematical model. What is known as a false negative is the likelihood that the mathematical model may overlook a true positive.

$$Arrival_{Mean} = \frac{1}{N}\sum_{i=1}^{n} IP^{Arrivaltime} ,$$

$$The\ IP\ address's\ inter - arrival\ time\ in\ a\ sliding\ window\ of\ 10\ s\ is\ shown\ by\ IP^{Arrival\ time}$$

$$T_h = \frac{TransferPacket_{size}}{Inter{-}Arrival_{attacker}} \quad (8)$$

$$T_h = TransferPacket_{size} * Frequencyofarrival \quad (9)$$

Table 3. Throughput computation for attack and regular scenarios

Inter-arrival time	Arrival frequency in Seconds	Throughput	Destination	Source	Label condition	Label
17.549695	8431.03	3.455	71.126.222.64	202.1.175.252	Normal	Normal Scenario
17.548384	2500.000	3.356	71.126.222.64	192.95.27.190	Normal	Normal Scenario
17.546908	467.301	1.128	71.126.222.64	192.120.148.227	Normal	Normal Scenario
17.544041	1139.061	31.168	71.126.222.64	40.75.89.172	Normal	Normal Scenario
17.537825	432.463	39.046	71.126.222.64	192.95.27.190	Normal	Normal Scenario
17.533944	857.684	556.771	71.126.222.64	51.81.166.201	Normal	Normal Scenario
17.531215	788.022	42.912	71.126.222.64	192.120.148.227	Normal	Normal Scenario
0.000150	6668.623	400117.400	71.126.222.64	192.95.27.190	Attack	Attack Scenario
0.020945	47.743	2864.629	71.126.222.64	51.81.166.201	Attack	Attack Scenario
0.000691	1446.992	86819.500	71.126.222.64	192.120.148.227	Attack	Attack Scenario
0.000119	8431.703	505902.200	71.126.222.64	202.1.175.252	Attack	Attack Scenario

$$Miss\ rate = \frac{FN}{(FN + TP)}\ , TP = 20038\ (predicted\ accurately), FN = 52$$

$$Miss\ rate = \frac{52}{20090} = 0.0025$$

The real-time Caida 2007 datasets, which include information on denial of service, are used as input for mathematical models. Mathematical models analyze the throughput and frequency of that specific information to identify which data is normal and which is an assault. Similar to how higher throughput equates to more processing time, processing time prevents legitimate clients from taking charge, meeting their processing needs, and allowing their data to sit in a queue indefinitely. Validation concerning the miss rate is also carried out to assess the accuracy of the mathematical model, taking into account the Caida dataset.**Figure 4** displays the experimental model's activity diagram.

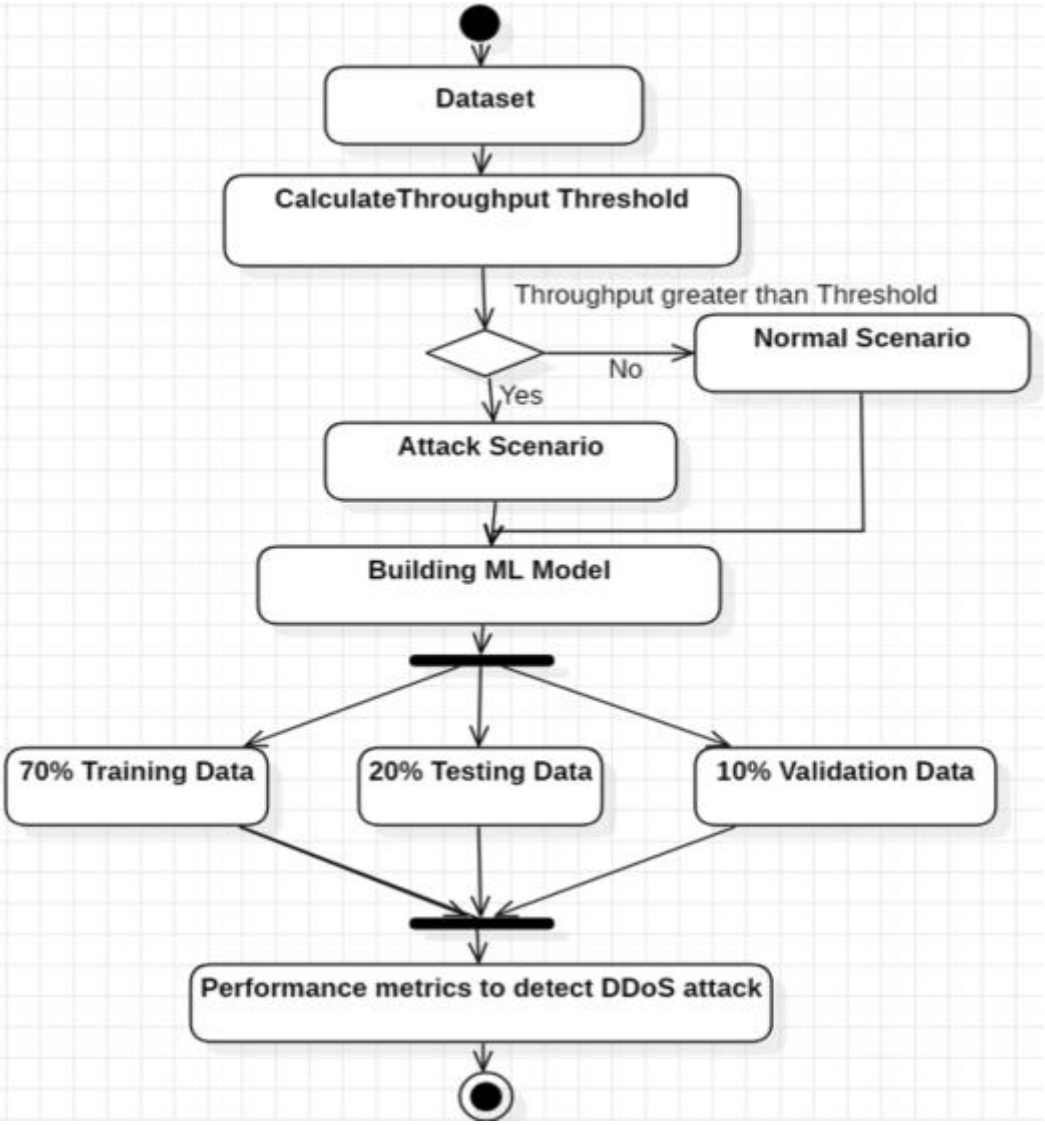

Figure 4 Experimental model's activity diagram

The Caida dataset is considered for determining the throughput threshold that will classify both normal and assault scenarios. The threshold is compared with the data throughput. If the throughput exceeds the threshold, it is categorized as an attack; otherwise, it is deemed normal.Afterward, the suggested model is further evaluated using ML models like LR and NB. The throughput threshold is determined by taking the median of the Caida dataset.LR and NB algorithms are used to build two ML models. LR is typically applied to prediction analysis. The LR method makes sense because the work's main objective in this study is to forecast DDoS attacks. For all features, NB generally assumes conditional independence. Consequently, the prediction can be off if some features are interdependent (as would be the case with an ample feature space).There are 20090 records in the original dataset, divided into 70:20:10 categories. In other words, 14063 records (70%) are utilized for training, 5425 records (20%) are utilized for testing, and the remaining 602 records (10%) are used for cross-validation.The data is tracked according to the following metrics: accurately diagnosed cases, cases that are misdiagnosed, sharpness, retention, frequency of completely false positives, percentage of instances categorized as positives, and coefficient of determination of mistake.The performance matrices to identify DDoS attack and the corresponding formula for accuracy, precision and recall formula are shown in the **Figure 5.**

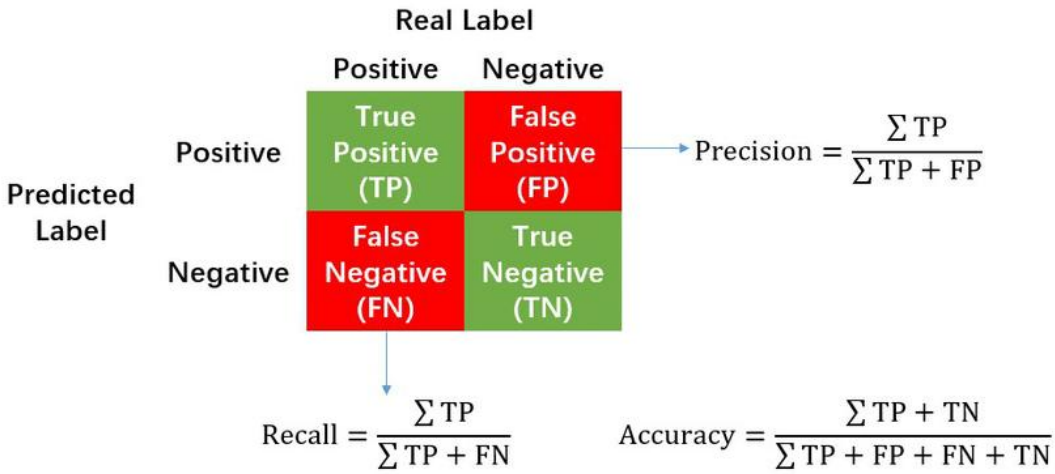

Figure 5.Computation of accuracy, recall and Precision in the confusion matrix

4. Results and Discussions

The experimental model's outcomes utilizing naive Bayes and logistic regression, two ML techniques, are shown in this section. The experiment outcomes are retrieved using the Weka tool. By subsampling the data, large datasets can also be utilized with non-incremental learning techniques. Weka also offers distributed data mining options that are compatible with Spark and Hadoop.The overview of the findings of the experimental model is displayed in **Table 6.**The accuracy ranges for LR and NB are 99–100% and 99–98%, respectively. As a result, LR produced superior outcomes than NB.While the MAE with NB is 0.007, 0.006, and 0.0163, the MAE with LR is 0, 0.0015, and 0.0017. Because LR's mean absolute error (MAE) value is lower than NB's, LR's findings are also superior.Utilizing the LR technique, the recall value in the attack scenario is 0.997, whereas in the usual case, it is 1.000. Using the NB technique, the recall value in the attack situation is 0.974, while in the typical case, it is 1.000. This indicates that while the recall value for the attack and regular scenario is significantly better in NB, it is less so in LR.It is also believed that the properties of NB are conditionally independent. Real data sets can approximate independence, even though they are never totally independent. In summary, NB has a lesser variance but a more considerable bias than LR. NB is a better classifier if the data set reflects the bias. LR and NBs are both types of linear classifiers. On the other hand, NB ascertains the formation of the data in light of the findings, whereas LR uses a direct functional form to provide a probability forecast.1.000 is the same precision value while utilizing NB and LR. Therefore, it is insufficient to identify DDoS with sufficient precision. Further factors like MAE, recall, and accuracy are necessary for the performance metrics analysis.

Table 6.The overview of the findings of the experimental model

Data	Total of all cases	Appropriately categorized cases	Class	ML algorithm utilized	Mean Absolute Error (MAE)	Recall	Precision	Accuracy
Training	14063	13929	Normal	NB	0.007	1.000	0.981	99.04
	14063	14063	Normal	LR	0	1.000	1.000	100
	14063	13929	Attack	NB	0.007	0.981	1.000	99.04
	14063	14063	Attack	LR	0	1.000	1.000	100

Test	5425	5385	Normal	NB	0.0061	1.000	0.986	99.26
	5425	5417	Normal	LR	0.0015	1.000	0.997	99.85
	5425	5385	Attack	NB	0.0061	0.985	1.000	99.26
	5425	5417	Attack	LR	0.0015	0.997	1.000	99.85
Validating	602	594	Normal	NB	0.0163	1.000	0.974	98.67
	602	601	Normal	LR	0.0017	1.000	0.997	99.83
	602	594	Attack	NB	0.0163	0.974	1.000	98.67
	602	601	Attack	LR	0.0017	0.997	1.000	99.83
LR is Logistic Regression and NB is Naïve Bayes								

5. Conclusion

Financial institutions are especially at risk because their data has significant monetary value. Selling the bank passwords and financial data that hackers have obtained can bring in enormous sums of money. Similarly, hackers can now access a larger attack surface due to banks' growing traces of digital technology.We want to detect DDoS attacks against other organizations and financial institutions using the Caida dataset. Attacks against the financial sector have been identified through the usage of ML algorithms. This research project used the Caida dataset to determine and assess the relationship between the requests' arrival times and throughput. The throughput is found to be inversely related to the inter-arrival time of the requests. Two models for identifying DDoS assaults have been put forth: one based on mathematics and the other on ML.Performance measures are assessed using ML approaches such as LR and NB, where logistic regression produces better results than Naive Bayes.It has also been observed that ML models perform marginally better than mathematical models. The mathematical model has 99.75% accuracy, while the ML model has 100% accuracy. The methodology presented in this paper makes DDoS attack identification more straightforward and more effective. It also illustrates how well ML algorithms work because a study compared Naïve Bayes with Logistic regression. Efficient analysis takes advantage of real-time datasets. Naive Bayes and Logistic regression were chosen because they produced good results.Mathematical and machine learning models must be evaluated against real-world threats. The results of this paper can also be applied to prevent memory management and firewall assaults. The model that is being given has a restriction in that it was developed using data from a single dataset. As such, a distributed dataset can be analyzed to guide future improvements.

References

[1] Sambangi, Swathi, and Lakshmeeswari Gondi. 2020. "A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection Using Multiple Linear Regression" *Proceedings* 63, no. 1: 51.

[2] Khader, R.; Eleyan, D. Survey of dos/ddos attacks in iot. Sustain. Eng. Innov. 2021, 3, 23–28.

[3] Hussain, F.; Abbas, S.G.; Husnain, M.; Fayyaz, U.U.; Shahzad, F.; Shah, G.A. IoT DoS and DDoS attack detection using ResNet. In Proceedings of the 2020 IEEE 23rd International Multitopic Conference (INMIC), Bahawalpur, Pakistan, 5–7 November 2020; pp. 1–6.

[4] Alanazi, F.; Jambi, K.; Eassa, F.; Khemakhem, M.; Basuhail, A.; Alsubhi, K. Ensemble Deep Learning Models for Mitigating DDoS Attack in Software-Defined Network. Intell. Autom. Soft Comput. 2022, 33, 2.

[5] Džaferović, E.; Sokol, A.; Abd Almisreb, A.; Norzeli, S.M. DoS and DDoS vulnerability of IoT: A review. Sustain. Eng. Innov. 2019, 1, 43–48.

[6] Ramalingam, H.; Venkatesan, V.P. Conceptual analysis of Internet of Things use cases in

Banking domain. In Proceedings of the TENCON 2019-2019 IEEE Region 10 Conference (TENCON), Kochi, India, 17–20 October 2019; pp. 2034–2039.

[7] George, A.; Ravindran, A.; Mendieta, M.; Tabkhi, H. Mez: An adaptive messaging system for latency-sensitive multi-camera machine vision at the iot edge. IEEE Access 2021, 9, 21457–21473.

[8] George, A.; Ravindran, A. Distributed middleware for edge vision systems. In Proceedings of the 2019 IEEE 16th International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT and AI (HONET-ICT), Charlotte, NC, USA, 6–9 October 2019; pp. 193–194.

[9] Mendieta, M.; Neff, C.; Lingerfelt, D.; Beam, C.; George, A.; Rogers, S.; Ravindran, A.; Tabkhi, H. A Novel Application/Infrastructure Co-design Approach for Real-time Edge Video Analytics. In Proceedings of the 2019 SoutheastCon, Atlanta, GA, USA, 10–13 March 2019; pp. 1–7.

[10] Xanthidis, D.; Nicholas, D. Evaluating internet usage and ecommerce growth in Greece. In Proceedings of the Aslib Proceedings; Emerald Group Publishing Limited: Bingley, UK, 2004.

[11] Ch, A.; Ch, R.; Gadamsetty, S.; Iwendi, C.; Gadekallu, T.R.; Dhaou, I.B. ECDSA-Based Water Bodies Prediction from Satellite Images with UNet. Water 2022, 14, 2234

[12] Liu, J.; Zhang, W.; Ma, T.; Tang, Z.; Xie, Y.; Gui, W.; Niyoyita, J.P. Toward security monitoring of industrial Cyber-Physical systems via hierarchically distributed intrusion detection. Expert Syst. Appl. 2020, 158, 113578.

[13] Fallows, D. The Internet and Daily Life; Pew Internet & American Life Project: Washington, DC, USA, 2004.

[14] Gupta, M.; Abdelsalam, M.; Khorsandroo, S.; Mittal, S. Security and Privacy in Smart Farming: Challenges and Opportunities. IEEE Access 2020, 8, 34564–34584.

[15] Alqahtani, A.S. Security threats and countermeasures in software defined network using efficient and secure trusted routing mechanism. Comput. Commun. 2020, 153, 336–341.

[16] Al-Ghamdi, A.; Al-Sulami, A.; Aljahdali, A.O. On the security and confidentiality of quantum key distribution. Secur. Priv. 2020, 3, 1–14.

[17] Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. Comput. Netw. 2020, 169, 107094.

[18] Jaafar, G.A.; Abdullah, S.M.; Ismail, S. Review of Recent Detection Methods for HTTP DDoS Attack. J. Comput. Netw. Commun. 2019, 2019, 1283472.

[19] Rahman, O.; Quraishi, M.A.G.; Lung, C.H. DDoS attacks detection and mitigation in SDN using machine learning. Proc. 2019 IEEE World Congr. Serv. Serv. 2019, 2642-939X, 184–189.

[20] Amjad, A.; Alyas, T.; Farooq, U.; Tariq, M. Detection and mitigation of DDoS attack in cloud computing using machine learning algorithm. ICST Trans. Scalable Inf. Syst. 2018, 6, 159834.

[21] Sreeram, I.; Vuppala, V.P.K. HTTP flood attack detection in application layer using machine learning metrics and bio inspired bat algorithm. Appl. Comput. Inform. 2019, 15, 59–66.

[22] Wang, J.; Liu, Y.; Feng, H. IFACNN: Efficient DDoS attack detection based on improved firefly algorithm to optimize convolutional neural networks. Math. Biosci. Eng. 2021, 19, 1280–1303.

[23] Chayomchai, A.; Phonsiri, W.; Junjit, A.; Boongapim, R.; Suwannapusit, U. Factors affecting acceptance and use of online technology in Thai people during COVID-19 quarantine time. Manag. Sci. Lett. 2020, 10, 3009–3016.

[24] Mhamane, S.S.; Lobo, L.M.R.J. Internet banking fraud detection using HMM. In Proceedings of the 2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12), Coimbatore, India, 26–28 July 2012.

[25] Alimolaei, S. An intelligent system for user behavior detection in Internet Banking. In Proceedings of the 2015 4th Iranian Joint

Congress on Fuzzy and Intelligent Systems (CFIS), Zahedan, Iran, 9–11 September 2015.

[26] Fang, L.; Li, Y.; Liu, Z.; Yin, C.; Li, M.; Cao, Z.J. A Practical Model Based on Anomaly Detection for Protecting Medical IoT Control Services against External Attacks. IEEE Trans. Ind. Inform. 2021, 17, 4260–4269.

[27] Using, N.; Learning, M. A Comprehensive Study of Anomaly Detection Schemes in IoT Networks Using Machine Learning Algorithms. Sensors 2021, 21, 8320.

[28] Gupta, B.B.; Chaudhary, P.; Chang, X.; Nedjah, N. Smart defense against distributed Denial of service attack in IoT networks using supervised learning classifiers. Comput. Electr. Eng. 2022, 98, 107726.

[29] Panigrahi, R.; Borah, S. A detailed analysis of CICIDS2017 dataset for designing Intrusion Detection Systems. Int. J. Eng. Technol. 2018, 7, 479–482.

[30] Doshi, R.; Apthorpe, N.; Feamster, N. Machine Learning DDoS Detection for Consumer Internet of Things Devices. In Proceedings of the 2018 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 24 May 2018; pp. 29–35

[31] Roopak, M.; Tian, G.Y.; Chambers, J. An Intrusion Detection System Against DDoS Attacks in IoT Networks. In Proceedings of the 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 6–8 January 2020; pp. 562–567.

[32] Saini, P.S.; Behal, S.; Bhatia, S. Detection of DDoS Attacks using Machine Learning Algorithms. In Proceedings of the 2020 7th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 12–14 March 2020; Volume 78, pp. 16–21.

[33] Aysa, M.H.; Ibrahim, A.A.; Mohammed, A.H. IoT Ddos Attack Detection Using Machine Learning. In Proceedings of the 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Istanbul, Turkey, 22–24 October 2020; pp. 1–7.

[34] Pande, S.; Khamparia, A.; Gupta, D.; Thanh, D.N.H. DDOS Detection Using Machine Learning Technique. In Recent Studies on Computational Intelligence; Studies in Computational Intelligence; Springer: Singapore, 2021; Volume 921

[35] Pokhrel, S.; Abbas, R.; Aryal, B. IoT Security: Botnet detection in IoT using Machine learning. arXiv 2021, arXiv:2104.02231.

[36] Chandrakala, S., and G. Revathy. "Success Stories for IoT-Enabled 6G for Prediction and Monitoring of Infectious Diseases with Artificial Intelligence." *6G-Enabled IoT and AI for Smart Healthcare*. CRC Press, 2023. 199-214.

[37] Liu, Z.; Thapa, N.; Shaver, A.; Roy, K.; Siddula, M.; Yuan, X.; Yu, A. Using Embedded Feature Selection and CNN for Classification on CCD-INID-V1—A New IoT Dataset. Sensors 2021, 21, 4834.

[38] Gaur, V.; Kumar, R. Analysis of Machine Learning Classifiers for Early Detection of DDoS Attacks on IoT Devices. Arab. J. Sci. Eng. 2022, 47, 1353–1374

[39] Mihoub, A.; Fredj, O.B.; Cheikhrouhou, O.; Derhab, A.; Krichen, M. Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques. Comput. Electr. Eng. 2022, 98, 107716.

[40] Gopi, R.; Sathiyamoorthi, V.; Selvakumar, S.; Manikandan, R.; Chatterjee, P.; Jhanjhi, N.Z.; Luhach, A.K. Enhanced method of ANN based model for detection of DDoS attacks on multimedia internet of things. Multimed. Tools Appl. 2021, 24, 26739–26757.

[41] 51 Prasad, A.; Chandra, S. VMFCVD: An Optimized Framework to Combat Volumetric DDoS Attacks using Machine Learning. Arab. J. Sci. Eng. 2022, 47, 9965–9983.

[42] Almaraz-Rivera, J.G.; Perez-Diaz, J.A.; Cantoral-Ceballos, J.A. Transport and Application Layer DDoS Attacks Detection to IoT Devices by Using Machine Learning and Deep Learning Models. Sensors 2022, 22, 3367

[43] Islam, U.; Muhammad, A.; Mansoor, R.; Hossain, M.S.; Ahmad, I.; Tageldin, E.; Khan, J.A.; Rehman, A.U.; Shafiq, M. Detection of Distributed Denial of Service (DDoS) Attacks in IOT Based Monitoring System of Banking Sector Using Machine Learning Models. Sustainability 2022, 14, 8374.

[44] Ismail, M.I.; Mohmand, H.; Hussain, A.A.; Khan, U.; Ullah, M.; Zakarya, A.; Ahmed, M.;

Raza, I.; Rahman, U.; Haleem, M. A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks. IEEE Access 2022, 10, 21443–21454.

[45] Amrish, R.; Bavapriyan, K.; Gopinaath, V.; Jawahar, A.; Vinoth, C.K. DDoS Detection using Machine Learning Techniques. J. IoT Soc. Mob. Anal. Cloud 2022, 4, 24–32.

[46] Aldweesh, A.; Derhab, A.; Emam, A.Z. Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. Knowl.-Based Syst. 2020, 189, 105124.

[47] Masdari, M.; Khezri, H. A survey and taxonomy of the fuzzy signature-based Intrusion Detection Systems. Appl. Soft Comput. J. 2020, 92, 106301.

[48] Bhuyan, M.H.; Bhattacharyya, D.K.; Kalita, J.K. Network anomaly detection: Methods, systems and tools. IEEE Commun. Surv. Tutor. 2013, 16, 303–336.

[49] Meng, W.; Li, W.; Su, C.; Zhou, J.; Lu, R. Enhancing trust management for wireless intrusion detection via traffic sampling in the era of big data. IEEE Access 2017, 6, 7234–7243.

[50] Singh, K.; Singh, P.; Kumar, K. Application layer HTTP-GET flood DDoS attacks: Research landscape and challenges. Comput. Secur. 2017, 65, 344–372. [Google Scholar] [CrossRef]

[51] O'Ree, A.J.; Obaidat, M.S. Security enhancements for UDDI. Secur. Commun. Netw. 2011, 4, 871–887.

[52] Zargar, S.T.; Joshi, J.; Tipper, D. A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks. IEEE Commun. Surv. Tutor. 2013, 15, 2046–2069.

[53] Kesavamoorthy, R.; Alaguvathana, P.; Suganya, R.; Vigneshwaran, P. Classification of DDoS attacks—A survey. Test Eng. Manag. 2020, 83, 12926–12932.

[54] Chang, R.K. Defending against flooding-based distributed denial-of-service attacks: A tutorial. IEEE Commun. Mag. 2002, 40, 42–51.

[55] Jazi, H.H.; Gonzalez, H.; Stakhanova, N.; Ghorbani, A.A. Detecting HTTP-based application layer DoS attacks on web servers in the presence of sampling. Comput. Netw. 2017, 121, 25–36.

[56] Behal, S.; Kumar, K.; Sachdeva, M. D-FACE: An anomaly based distributed approach for early detection of DDoS attacks and flash events. J. Netw. Comput. Appl. 2018, 111, 49–63.

[57] Wang, C.; Miu, T.T.; Luo, X.; Wang, J. SkyShield: A sketch-based defense system against application layer DDoS attacks. IEEE Trans. Inf. Forensics Secur. 2018, 13, 559–573.

[58] Aamir, M.; Zaidi, S.M.A. Clustering based semi-supervised machine learning for DDoS attack classification. J. King Saud Univ. Comput. Inf. Sci. 2019, 33, 436–446.

[59] 1Islam, U.; Muhammad, A.; Mansoor, R.; Hossain, M.S.; Ahmad, I.; Eldin, E.T.; Khan, J.A.; Rehman, A.U.; Shafiq, M. Detection of distributed denial of service (DDoS) attacks in IOT based monitoring system of banking sector using machine learning models. Sustainability 2022, 14, 8374.

[60] 40 Almaraz-Rivera, J.G.; Perez-Diaz, J.A.; Cantoral-Ceballos, J.A. Transport and Application Layer DDoS Attacks Detection to IoT Devices by Using Machine Learning and Deep Learning Models. Sensors 2022, 22, 3367.

[61] 39 Ahuja, N.; Singal, G.; Mukhopadhyay, D.; Kumar, N. Automated DDOS attack detection in software defined networking. J. Netw. Comput. Appl. 2021, 187, 103108.

[62] 38Dehkordi, A.B.; Soltanaghaei, M.; Boroujeni, F.Z. The DDoS attacks detection through machine learning and statistical methods in SDN. J. Supercomput. 2021, 77, 2383–2415.

[63] 37Awan, M.J.; Farooq, U.; Babar, H.M.A.; Yasin, A.; Nobanee, H.; Hussain, M.; Hakeem, O.; Zain, A.M. Real-Time DDoS Attack Detection System Using Big Data Approach. Sustainability 2021, 13, 743.

[64] 36Priya, S.S.; Sivaram, M.; Yuvaraj, D.; Jayanthiladevi, A. Machine learning based DDoS detection. In Proceedings of the 2020 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 5–7 March 2020; pp. 234–237.

[65] 35Pubudu, R.D.; Indrasiri, L.; Lee, E.; Rupapara, V.; Rustam, F.; Ashraf, I. Malicious Traffic Detection in IoT and Local Networks Using Stacked Ensemble Classifier. Comput. Mater. Contin. 2022, 71, 489–515.

[66] 34Yungaicela-Naula, N.M.; Vargas-Rosales, C.; Perez-Diaz, J.A. SDN-Based Architecture for Transport and Application Layer DDoS Attack Detection by Using Machine and Deep Learning. IEEE Access 2021, 9, 108495–108512.

[67] Salem, O.; Alsubhi, K.; Shaafi, A.; Gheryani, M.; Mehaoua, A.; Boutaba, R. Man-in-the-Middle Attack Mitigation in Internet of Medical Things. IEEE Trans. Ind. Inform. 2022, 18, 2053–2062.

[68] Fang, L.; Li, Y.; Liu, Z.; Yin, C.; Li, M.; Cao, Z.J. A Practical Model Based on Anomaly Detection for Protecting Medical IoT Control Services against External Attacks. IEEE Trans. Ind. Inform. 2021, 17, 4260–4269.

[69] Gupta, D.; Gupta, M.; Bhatt, S.; Tosun, A.S. Detecting Anomalous User Behavior in Remote Patient Monitoring. In Proceedings of the 2021 IEEE 22nd International Conference on Information Reuse and Integration for Data Science (IRI), Las Vegas, NV, USA, 10–12 August 2021; pp. 33–40.

[70] Using, N.; Learning, M. A Comprehensive Study of Anomaly Detection Schemes in IoT Networks Using Machine Learning Algorithms. Sensors 2021, 21, 8320.

[71] Saeedi, K. Machine Learning for Ddos Detection in Packet Core Network for IoT. Master's Thesis, Luleå University of Technology, Luleå, Sweden, 2019.

[72] Tahir Ullah, K. Internet of Things (IOT) systems and its security challenges. Int. J. Adv. Res. Comput. Eng. Technol. 2019, 8, 12.

[73] Kamruzzaman, M.M. New Opportunities, Challenges, and Applications of Edge-AI for Connected Healthcare in Smart Cities. In Proceedings of the 2021 IEEE Globecom Workshops (GC Wkshps), Madrid, Spain, 7–11 December 2021.

[74] Jegadeesan, S.; Azees, M.; Ramesh Babu, N.; Subramaniam, U.; Almakhles, J.D. EPAW: Efficient Privacy Preserving Anonymous Mutual Authentication Scheme for Wireless Body Area Networks (WBANs). IEEE Access 2020, 8, 48576–48586.

[75] Oppliger, R.; Rytz, R.; Holderegger, T. Internet banking: Client-side attacks and protection mechanisms. Computer 2009, 42, 27–33.

[76] Zachos, G.; Essop, I.; Mantas, G.; Porfyrakis, K.; Ribeiro, J.C. An Anomaly-Based Intrusion Detection System Internet of Medical Things Networks. Electronics 2021, 10, 2562.

[77] Lange, T.; Kettani, H. On Security Threats of Botnets to Cyber Systems. In Proceedings of the 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 7–8 March 2019; pp. 176–183.

[78] Aski, V.; Dhaka, V.S.; Kumar, S.; Parashar, A.; Ladagi, A. A multi-factor access control and ownership transfer framework for future generation healthcare systems. In Proceedings of the 2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC), Waknaghat, India, 6–8 November 2020; pp. 93–98.

[79] Mehmood, M.; Javed, T.; Nebhen, J.; Abbas, S.; Abid, R.; Bojja, G.R.; Rizwan, M. A hybrid approach for network intrusion detection. Comput. Mater. Contin. 2021, 70, 91–107.

[80] Ramapatruni, S.; Narayanan, S.N.; Mittal, S.; Joshi, A.; Joshi, K. Anomaly Detection Models for Smart Home Security. In Proceedings of the 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), Washington, DC, USA, 27–29 May 2019; pp. 19–24.

[81] Hameed, M.; Yang, F.; Ghafoor, M.I.; Jaskani, F.H.; Islam, U.; Fayaz, M.; Mehmood, G. IOTA-Based Mobile Crowd Sensing: Detection of Fake Sensing Using Logit-Boosted Machine Learning Algorithms. Wirel. Commun. Mob. Comput. 2022, 2022, 6274114.

[82] Kaushik, I.; Sharma, N. Black hole attack and its security measure in wireless sensors networks. In Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's; Springer: Cham, Switzerland, 2020; Volume 1132.

[83] Dilraj, M.; Nimmy, K.; Sankaran, S. Towards Behavioral Profiling Based Anomaly Detection for Smart Homes. In Proceedings of the TENCON 2019–2019 IEEE Region 10 Conference (TENCON), Kochi, India, 17–20 October 2019; pp. 1258–1263.

[84] Javeed, D.; Khan, M.T.; Ahmad, I.; Iqbal, T.; Badamasi, U.M.; Ndubuisi, C.O.; Umar, A. An efficient approach of threat hunting using memory forensics. Int. J. Comput. Netw. Commun. Secur. 2020, 8, 37–45.

[85] Javeed, D.; Gao, T.; Khan, M.T.; Shoukat, D. A hybrid intelligent framework to combat sophisticated threats in secure industries. Sensors 2022, 22, 1582.

[86] Shaikh, H.; Khan, M.S.; Mahar, Z.A.; Anwar, M.; Raza, A.; Shah, A. A conceptual framework for determining acceptance of internet of things (IoT) in higher education institutions of Pakistan. In Proceedings of the 2019 International Conference on Information Science and Communication Technology (ICISCT), Karachi, Pakistan, 9–10 March 2019; pp. 1–5.

[87] Huang, K.; Yang, L.X.; Yang, X.; Xiang, Y.; Tang, Y.Y. A Low-Cost Distributed Denial-of-Service Attack Architecture. IEEE Access 2020, 8, 42111–42119