

RESEARCH PROPOSAL

A Lightweight System for Real-Time DDOS Attack Detection In Cloud Networks

Name: Riddhi Damjibhai Mendpara

Student No: 2518862

Lecturer: Dr. Seena Joseph

Table of Contents.

Abstract	4
1. Introduction.....	4
1.1 Background and Context.....	5
1.2 Research Problem	5
1.3 Research Aim.....	6
1.4 Research Objectives.....	6
1.5 Research Significance.....	6
2. Literature Review.....	7
2.1 Introduction to the Literature Review.....	7
2.2 Thematic Organisation of Literature.....	7
2.2.1 Supervised Machine Learning Techniques.....	7
2.2.2 Unsupervised and Clustering-Based Techniques.....	8
2.2.3 Deep Learning Methods.....	9
2.2.4 Lightweight and Real-Time Detection Systems	10
2.3 Key Contributions and Research Gaps	11
2.4 Theoretical and Technical Frameworks.....	11
2.5 Relation to the Proposed Study.....	12
2.6 Literature Summary	12
3. Research Methodology	12
3.1 Research Methods.....	12
3.1.1 Overview of Research Methodology	12
3.1.2 Research Strategy.....	13
3.2 System Architecture and Design.....	14
3.3 Data Collection Table	15

3.4 Proposed Framework	16
3.5 Data Analysis and Evaluation Methods	16
3.6 Software Requirements	17
3.7 Hardware Requirements.....	17
3.8 Ethical Considerations	18
3.9 Summary	18
4. Expected Outcome	18
5. Project Plan	19
6. Conclusion	20
Reference List	21

Abstract

The availability of cloud computing at high rates has highly exposed the digital infrastructure to Distributed Denial-of-Service attacks (DDoS). According to such attacks, the availability of services is disrupted because the network resources are overloaded, resulting in financial losses and the establishment of operations. Although the current machine learning-based detection systems are highly accurate, they are computationally intensive and therefore cannot be used in real time in highly resource-constrained settings like small and medium-sized enterprises (SMEs). This study will demonstrate the design and development of a lightweight and real-time DDoS detector system, designed to work in the cloud context. The system combines effective machine learning algorithms with a modular framework made of machine learning-based traffic monitoring, analysis, and alerting modules and response modules. The system will be simulated over a Streamlet-based environment to offer real-time detection and visualization of the system using the BCCC-CIC Packet Cloud DDoS 2024 data set.

1. Introduction

1.1 Background and Context

Cloud computing has transformed the process of organisations' storage, processing, and management of data. Nevertheless, this change has made new security threats as well, specifically the Distributed Denial-of-Service (DDoS) attacks. These attacks are meant to use up network resources, rendering services unusable to legitimate persons. As it is emphasized in the given presentation (page 4), DDoS attacks have been growing out of proportion, and it is reported that they have increased by more than 166 percent over the last few years. Traditional detection systems have become ineffective with the growing sophistication of attacks, both in the use of multi-vector approaches to attacks and the use of ML models in attack management.

The vulnerabilities of cloud environments are especially reflected by the shared nature of infrastructure and dynamism in scaling. Attackers take advantage of these capabilities to create huge traffic quantities, crippling systems. In addition, the conventional security systems like Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) are mostly perimeter-based and are unable to intercept the internal east-west traffic on the clouds.

1.2 Research Problem

In spite of the massive improvements made in the area of cybersecurity, the current DDoS detection systems are still subjected to a number of critical challenges, which constrain their usability in cloud reality. Most new methods of detection are based on complicated machine learning or deep learning models and might demand computer resources and substantial processing capability. This renders them inappropriate to real-time implementation, particularly on dynamic cloud architectures that require immediate response. Despite this, the systems find it difficult to perform effectively under resource-scarce operations like small and medium-sized enterprises (SMEs), which do not have the infrastructure to implement expensive security solutions.

The other key weakness is the inability of traditional systems to observe and apprehend domestic cloud communication, specifically east-west communication between services. According to the presentation (page 5), SMEs need light and cheap solutions. Besides, the research gap identifies the absence of combined and comprehensive detection and response frameworks, which are efficient and can be adopted in reality.

1.3 Research Aim

The research aim is to design, develop, and test a lightweight real-time cloud network-based DDoS detection system which will guarantee a high detection rate with low computational load and is deployable to a constrained resource environment.

1.4 Research Objectives

No.	Objective
1	To analyse existing DDoS detection techniques and identify key limitations in performance, scalability, and real-time applicability in cloud environments
2	To select the efficient machine learning algorithms which is suitable for real-time DDoS detection in cloud systems
3	To design and demonstrate a scalable cloud-based detection system architecture for monitoring, analysis, and response components for cloud networks
4	To demonstrate a functional prototype using Python and Streamlit for real-time DDoS detection and interactive visualisation of network traffic
5	To evaluate the system performance by using multiple metrics such as accuracy, precision, recall, F1-score, and resource utilisation
6	To compare the proposed system performance with traditional detection methods for efficiency, accuracy, and scalability

1.5 Research Significance

This study will fill the gap between a high-performance model and the practical use by contributing towards the creation of a lightweight and cost-effective detection mechanism. The developed system is a balanced system that will promote increased use of proper countermeasures to DDoS attacks in practical cloud settings because it will be accessible and increase security. Such aim is also important because the study focuses on overcoming practical

barriers in order to accurately detect DDoS in cloud-based environments, such as cost, scalability, and efficiency. The majority of the existing attack detection mechanisms are based on resource-intensive models, impractical for real-time deployment in many on-site and large-scale dynamic cloud architectures. By focusing on efficiency and scalability, the designed system will be able to handle growing traffic throughout the network without significant performance degradation.

2. Literature Review

2.1 Introduction to the Literature Review

This literature review critically analyses the available research on DDoS detection in cloud-based environments with a critical interest to the main trends, methods, and gaps in the research. It addresses the tendency toward the increased application of machine learning and data-driven approaches to dealing with more sophisticated and large-scale attacks. The review analyses the performance of these approaches in the areas of scalability, efficiency, and applicability in real-time in any practical situation.

The latest literature within the past five to seven years is limited to displaying the relevance to the current developments in cybersecurity. It encompasses key sub-areas, such as supervised and unsupervised learning, deep learning models, and lightweight detection systems. There are other issues that are peculiar to cloud environments that are considered in the review, including distributed infrastructure, volume of traffic, and internal network communication.

2.2 Thematic Organisation of Literature

2.2.1 Supervised Machine Learning Techniques

Supervised machine learning models have also been extensively applied in the identification of DDoS attacks because they are used to distinguish network traffic using labelled datasets. One of the most accurate algorithms in detecting malicious traffic patterns is the Decision Trees, Random Forests, Support Vector Machines (SVM), and Logistic Regression algorithms [1]. Random Forest specifically has been identified with high levels of strength and the capacity to deal with high volumes of data consisting of more than a single feature.

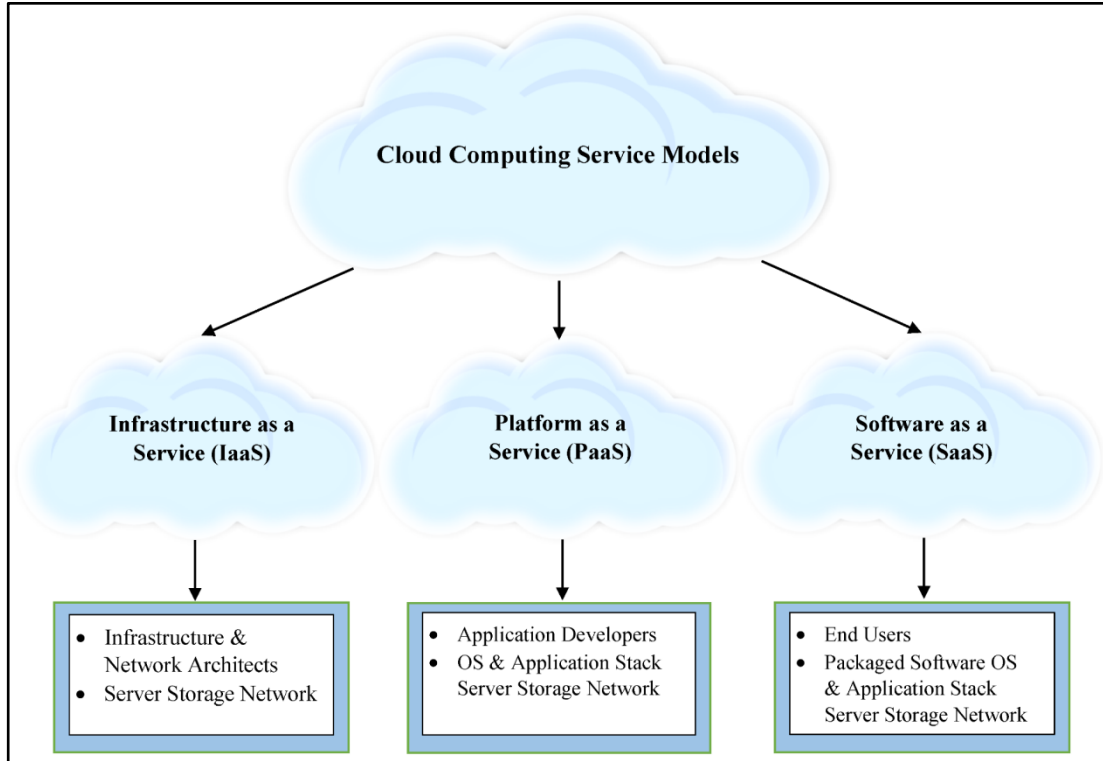


Figure 2.1: ML algorithms in cloud computing [2]

Nevertheless, the models are frequently computationally intensive to train and test, even when they have proven to be effective. Besides, the state of their performance is much more reliant on the quality and balance of the dataset. In a real-time system, the complexities involved in models spread latencies that may slow down faster detection, and so are inappropriate in time-sensitive applications.

2.2.2 Unsupervised and Clustering-Based Techniques

Unsupervised learning methods, especially clustering methods like K-means and K-medoids, are also commonly applied in the detection of anomalies in network traffic modeling. These methods do not require labelled data, and therefore, they have high capabilities of detecting unknown or novel patterns of DDoS attacks. Clustering techniques are capable of identifying anomalies of normal traffic behaviour by grouping similar data points according to similarity of features, which can be an indication of malicious actions [3]. It renders them especially efficient in dynamic cloud environments, wherein attack signatures are constantly changing and cannot always be defined.

Nevertheless, even though they are flexible, the unsupervised methods have a number of shortcomings. They are usually less detectable than their supervised learning equivalents in that they do not use classification boundaries as well, but rather assumptions on how data are distributed. Also, clustering algorithms tend to have high false positives since not every anomaly is associated with an actual attack. The next important issue is the choice of the best parameters, including the number of clusters, which has a direct impact on the performance. Such limitations decrease their accuracy in real-time DDoS detection systems, particularly when accurate classification is needed.

2.2.3 Deep Learning Methods

Over the past few years, deep learning methods have attracted significant attention due to their detection capabilities in complex and large-scale DDoS attacks. DNNs, like Convolutional Neural Networks and Recurrent Neural Networks, can automatically infer high-level features out of raw network traffic data, avoiding manual feature engineering [4]. The models are very useful in the detection of multi-vector and changing patterns of attacks because they can learn complex relationships with vast data. Consequently, deep learning methods can tend to reach higher detection accuracy than classical machine learning models.

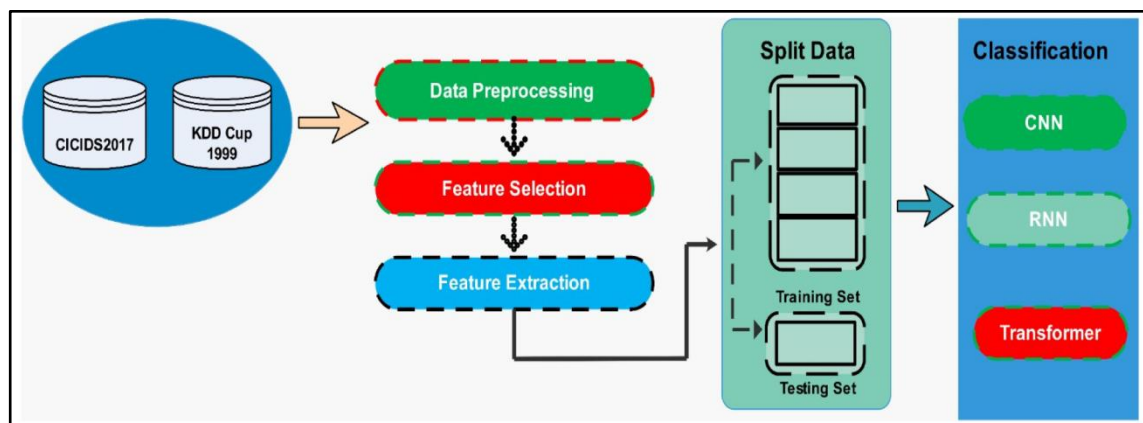


Figure 2.2: Deep learning techniques in attack detection [5]

Even though they have benefits, deep learning approaches have a number of practical challenges. They are also computationally intensive (high-performance GPUs and high memory capacity), which makes them more expensive to implement. These models also require significant quantities of labeled training data, which is not always available. They are also not suitable in latency-sensitive environments, such as real-time detection, because their architecture is

complex, and hence the training and inference time is longer than the source code. Therefore, deep learning is considered to be very high-performing, but not usually feasible on extremely lightweight and resource-intensive cloud platforms like those supported by SMEs.

2.2.4 Lightweight and Real-Time Detection Systems

The research and development of lightweight DDoS detectors, criticized as a real-time application, has become a proposed research topic in recent years. Lightweight methods are normally based on simplified machine learning models, feature selection methods, and hybrid detection methodologies in order to limit the processing workload whilst preserving reasonable levels of performance.

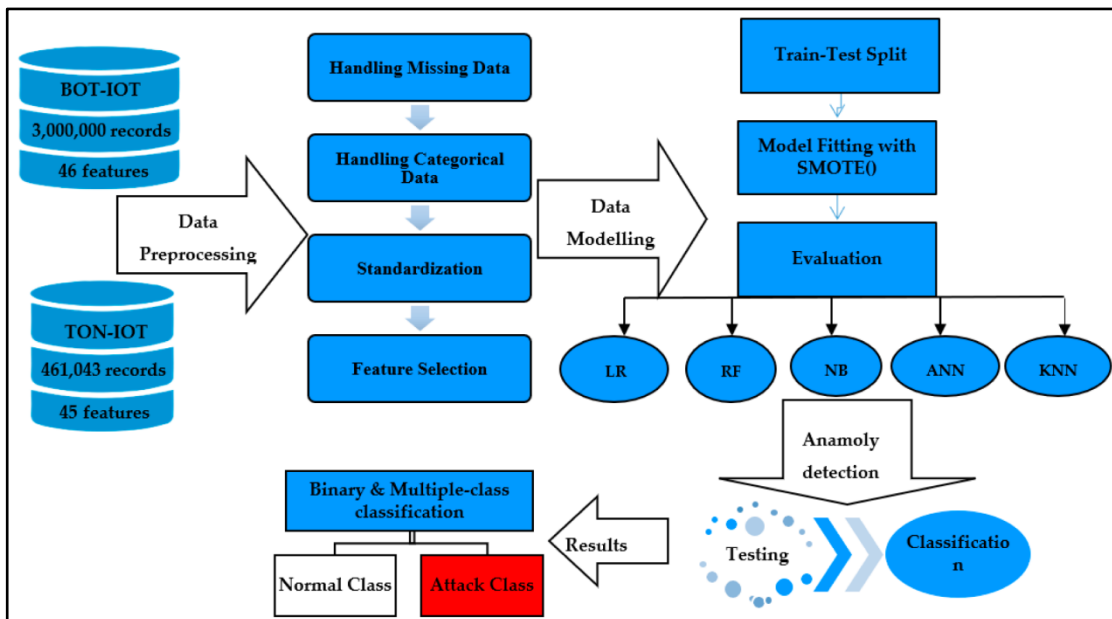


Figure 2.3: Lightweight Model for DDoS Attack Detection [6]

Irrespective of those issues, lightweight detection systems are a good avenue to follow in future research since they respond to the practicality of the traditional and deep learning methods in use, and the scalability and efficiency of the deployment within a real-world cloud environment becomes achievable. The second solution is the improvement of real-time detection through new technologies such as Extended Berkeley Packet Filter (eBPF) and Express Data Path (XDP), along with the optimization of algorithms. These technologies allow processing packets as low as the kernel level which makes the difference in behavioral decision smaller and increases

throughput. However, integrating low-level technologies into machine learning models is an intricate task that requires specialized skills.

2.3 Key Contributions and Research Gaps

The available literature has contributed immensely to DDoS detection. The next evolution of deep learning has brought the sphere to a new stage due to the possibility of addressing intricate and multi-layered attacks. The Supervised models learning have proved to be highly accurate, whereas unsupervised techniques have provided the flexibility in the identification of uncategorized attack patterns.

However, several significant gaps exist:

- Computationally expensive, most high-accuracy models cannot be deployed in real time and are inappropriate.
- Poor emphasis on lightweight systems to accommodate SMEs.
- Absence of combined detection and response systems.
- Lack of assessment in the actual cloud platform.

A lot of research is done on the accuracy of detection without paying attention to practical implementation factors like cost, scalability, and availability of resources. This puts a distance between theoretical development and practical usefulness.

2.4 Theoretical and Technical Frameworks

DDoS detection systems run on the theoretical basis of classification and anomaly detection. Categorical Network traffic. The classification models are used to group network traffic into classes that are outliers or normal. An anomaly detector is used to detect a deviation or anomaly from the expected behaviour. Technically, most machine learning programs, such as Decision Trees, Random Forest, Support Vector machines, and Logistic Regression, are very common. Some data preprocessing methods, like feature selection, normalisation, and dimensionality reduction, enhance model performance and efficiency [7]. Measurements such as the accuracy, precision, recall, F1-score, and ROC-AUC are employed to measure model effectiveness. Also, Python and Scikit-learn are tools that can be used to implement. XDP and eBPF are both network-level technologies that can be used to improve real-time processing of packets. Nonetheless, there is a major issue of having lightweight models that are effectively processed.

2.5 Relation to the Proposed Study

Unlike traditional DDoS mitigation approaches that separate detection from response, this research offers a novel end-to-end DDoS mitigation system where both mechanisms are integrated. The study provides a realistic and recent performance evaluation on a reliable dataset. This system is efficient, scalable and well-suited to a cloud environment. A lightweight architecture that fits resource-constrained settings such as small and medium-sized enterprises (SMEs). The proposed study is based on the current research since it offers solutions to the main limitations of efficiency, scalability, and real-time applicability. Although a majority of earlier works involve enhancing the detection accuracy, this work will focus on creating a lightweight and practical solution that can be deployed in the real world [8]. The proposed system encompasses effective machine learning models that compromise performance with minimal computational needs. The Streamlit- or Streamlited-based interface is also being added, which makes this application useful because one can visualize and interact with it in real time.

2.6 Literature Summary

The state of the art in DDoS detection has greatly improved through various machine learning and data driven techniques fitted for cloud deployment [6]. While supervised models give us high accuracy, unsupervised and deep learning techniques is more flexible in detecting complex attack patterns. Solutions such as eBPF and XDP use emerging technologies to do so dynamically. But there are still some critical challenges to be resolved, such as large computational costs, low scalability and bad suitability for resource limited systems. This paper provides an insight to overcome these problems by developing a compact and efficient DDoS detection system for cloud environments. This study develops an approach that employs machine learning algorithms alongside a modular architecture and real-time simulation of processes, resulting in concurrent, scalable solutions to perform detection with deployable methodologies.

3. Research Methodology

3.1 Research Methods

3.1.1 Overview of Research Methodology

This research study uses a quantitative research approach because of the analysis of network traffic numerical data for the classification of network traffic with the occurrence of Distributed

Denial-of-Service (DDoS) attacks. Therefore, the use of the quantitative approach is suitable because the variables on which the study is based are measurable such as size of packet, flow duration and traffic frequency for the classification of network behaviour. Also in order to assess the model performance the statistical evaluation metrics such as accuracy, precision, recall and F1-score are used. In order to determine the model performance, statistical evaluation measures like accuracy, precision, recall, and F1-score will be utilized. A quantitative approach is used to provide objectivity, reproducibility, and the possibility to compare various machine learning models successfully. Given that the study aims to create and test a detection system with the help of actual data, quantitative analysis will be a solid tool to confirm the efficiency of the solution options.

3.1.2 Research Strategy

The software development feature is to develop a lightweight DDoS detection system with several modules, such as traffic monitoring, feature extraction, machine learning-based detection, alert generation, and response mechanisms [9]. To ensure a real-time interaction and visualisation, the system will be implemented in Python and embedded into an interface based on Streamlit. The experimental approach is to test the system with an actual data set in the simulated experiment. The data will be applied in batches to simulate real-time network traffic. Training and testing of various machine learning models will be undertaken to identify the best and most effective method. This plan is suitable as it permits the premeditated testing, comparison, and confirmation of outcomes under controlled circumstances.

3.2 System Architecture and Design

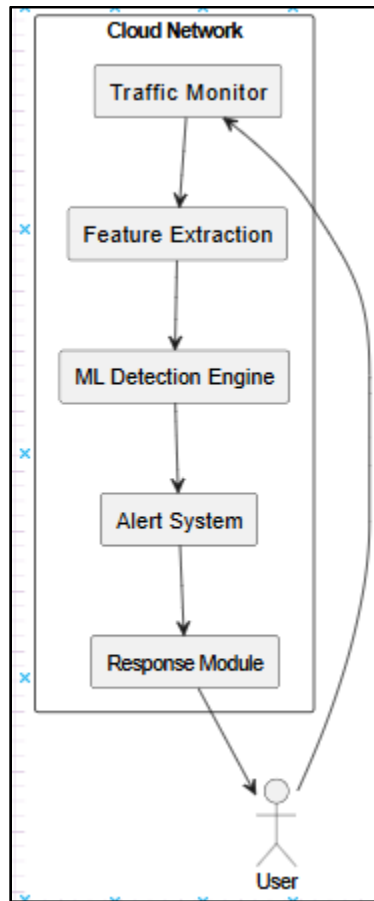


Figure 3.1: Flow chart of system architecture and design

The diagram of the proposed system is based on the modular architecture of the system that allows improving the scalability, flexibility, and processing efficiency, as the workflow is broken down into separate functional elements. The Traffic Monitoring Module reads and broadcasts the network traffic information on the dataset sequentially to re-create the conditions in real-time. This will give an incessant data flow to the system [10]. The raw traffic data is then fed into the Feature Extraction Module, which extracts the features like packet size, protocol type, and flow period, which are later important when performing the identification of a deviant pattern. After this, the Preprocessing Module carries out necessary functions such as data cleaning, missing values, normalisation, and feature selection. These are useful in enhancing data quality and dimensionality reduction, which leads to better and more efficient model performance. These modules collectively comprise the preliminary stages of the system as they guarantee that the

data received is in the right format, pertinent and optimised in its form before being handed over to the detection engine that carries out additional analysis.

3.3 Data Collection Table

Parameter	Description
Dataset Name	BCCC-CICPacket Cloud DDoS 2024
Source	Kaggle
Type	Network traffic
Format	Packet-level
Size	Large-scale dataset
Features	IP, packet size, protocol, flow duration
Labels	Attack / Normal
Purpose	Model training and evaluation

Table 1: Data collection table

The dataset BCCC-CICPacket Cloud DDoS 2024 is a large-scale dataset of network traffic collected through the Kaggle platform and is specifically configured to conduct research in the area of cybersecurity and DDoS indicators detection. It has packet-level information, which includes major characteristics like IP addresses, packet size, protocol type, and flow duration, which are crucial in the analysis of network behavior [11]. The data are classified as attack and normal traffic, which makes it possible to train the supervised machine learning models. It is big enough to guarantee a sufficient amount of information to test the model and conduct a performance test. In general, this data set is very appropriate for developing and testing real-time DDoS detection systems in cloud systems.

3.4 Proposed Framework

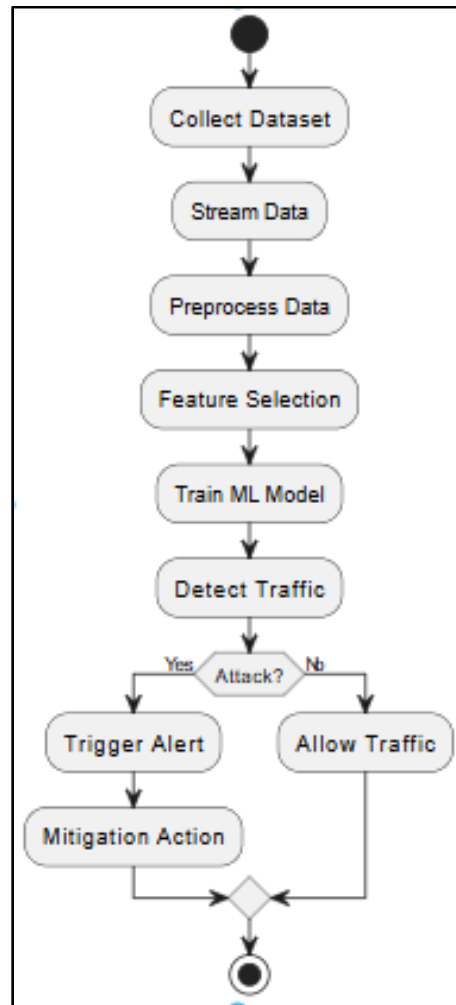


Figure 3.2: proposed system framework

The figure shows the diagram of a DDoS detection system. It commences with the collection of the data sets and streaming of data to generate simulated real-time traffic. The data is preprocessed, followed by the refining of the data by means of feature selection, and subsequently training a machine learning model [12]. The learnt model identifies traffic and decides whether it is an attack. When an attack is detected, an alarm goes off, and remedial measures are implemented. Otherwise, there is normal traffic traffic and the process is completed effectively.

3.5 Data Analysis and Evaluation Methods

Data analysis and evaluation during this research have a systematic process so that DDoS can be identified properly and effectively. First, it is preprocessed, eliminating gaps, inconsistencies or

duplicates of the data, to enhance the quality of the data. The techniques of feature scaling, like normalisation, are used in order to normalize the data in such a way that all features play an equal role in the model. The dimensionality is further reduced through the feature selection techniques, which contribute to the enhancement of computational efficiency and performance of the model.

After preprocessing, the data is separated into training and testing samples, which allows for a reliable evaluation. Several machine learning algorithms, such as Decision Tree, Random Forest, and Logistic Regression, are trained with the training data and tested on unknown data in order to check their efficiency. The dynamics of the models are measured with the help of a few metrics [13]. Accuracy measures the overall correctness, whereas precision and recall measure the aptitude of the model to be correct in recognizing attacks. These two are offset by the F1-score and the ROC-AUC, which measure the performance of classification. Also, the detection latency and resource utilisation are measured to make sure that the system is running effectively under conditions of real-time operation.

3.6 Software Requirements

The suggested system will be based on the potential of different software and technologies to facilitate optimal development, analysis, and deployment. Python is chosen as the main programming language because it has a powerful data science and machine learning ecosystem. The data manipulation and numerical processing will be performed with Libraries like Pandas and NumPy, and machine learning models will be implemented with the assistance of Scikit-learn. Matplotlib will help in data visualisation and interpretation of the results [14]. Streamlit is selected as the visualisation graphics to develop an interactive and real-time user interface to track the detection results. Jupyter Notebook and Visual Studio Code will be used as the coding and experimentation environment. Also, version control will be maintained with Git to maintain code. The combination of these tools is a guarantee of scalability, flexibility, and good performance of the system.

3.7 Hardware Requirements

The standard computing environment will be used to develop and test the proposed system to provide access and functionality. It demands at least 16GB of RAM as well as a multi-core CPU

to process data and run machine learning smoothly. It may have an optional graphics card to improve performance, but it is not necessary because of the lightweight models. In response, the researcher deliberately does not use the resources provided by cloud computing because the aim is to create a system that can work well on local computers [15]. This model promotes the SMEs and resource-limited environments by guaranteeing minimal deployment, low cost, and low hardware dependency.

3.8 Ethical Considerations

The data on which it was based is publicly accessible and has no personally recognizable information, so it will not violate the rules of data privacy. The study will make sure that all the information will be used in pure academic intentions and that findings will be presented openly and truthfully [16]. The system will also be used for the detection and response without causes a real system or networks. There will be ethical approvals that shall be adhered to as required by the institution.

3.9 Summary

The research methodology has been involved a combination of a quantitative data approach, software development, and experimental methods for the design and test a lightweight system of DDoS detection. Methods and materials used are well explained and justified to support the objectives of the research and address the weaknesses witnessed in the current approaches. The real-world data and the effective machine learning models, and a simulation based on Streamlit are all designed to make the system practical and effective.

4. Expected Outcome

The anticipated findings of this study are to come up with an effective and viable solution to detect DDoS within cloud environments. Firstly, the paper should provide a real-time lightweight system of detection that will be able to monitor network traffic in real-time and can detect possible attacks with minimal delay [7]. This avoids delay in response and mitigation, which is vital in ensuring that service is not disrupted. The system will attain a high detection rate with a low resource consumption rate, which will solve a significant constraint of current models that consume a lot of resources. The system will enable the strike of a balance between performance

and efficiency using the lightweight machine learning algorithms and optimised data processing techniques [17]. This is critical in a real-time environment in which slight delays may cause tremendous damage.

5. Project Plan

Task/Month	Feb 01,2026	Mar 06,2026	Apr 01,2026	May 08,2026	Jun 01,2026	July 01,2026	Aug 01,2026	Sep 01,2026	Oct 01,2026	Nov 01,2026	Dec 01,2026
Choose Topic											
Topic Preseantation											
Literature Review											
Proposal Submission											
Research Design											
Ethics Approval											
Data Collection											
Data Analysis											
Dissertation Writing											
Proofreading & Editing											
Final Submission											

6. Conclusion

The research provides a lightweight and efficient method of identifying DDoS attacks within cloud environments through the combination of machine learning methods and real-time data processing. This paper witnesses the major constraints of the current systems, like large consumptions and the unfeasibility of scaling, concentrating on low-resource and workable remedies. The system is designed to guarantee real-time detection, real-time usability, and real-time performance monitoring with a modular architecture and a simulation of the system, using Streamlit. The applicability of the related datasets and various assessment measures enhances the validity of the findings. All in all, the given solution helps to create a scalable, affordable, and deployable DDoS detection system that is applicable to newer cloud infrastructures, and especially SMEs will benefit.

Reference List

- [1] Papalkar, R.R., Alvi, A.S., Ali, S., Awasthy, M. and Kanse, R., 2023. An optimized feature selection guided light-weight machine learning models for DDoS attacks detection in cloud computing. In *Artificial Intelligence, Blockchain, Computing and Security Volume 1* (pp. 975-982). CRC Press.
- [2] Doan, V.T., 2025. *Research and Implementation of a Network Attack Detection and Classification System using Suricata IDS Integrated with Artificial Intelligence* (Doctoral dissertation, Vietnam-Korea University of Information and Communication Technology).
- [3] Kumar, N.S., Sai, M.V., Yadav, M.S.S. and Nagaraju, A.S., 2025, October. Real-Time Threat Detection in Networks Using Machine Learning: A Predictive Approach to Cybersecurity. In *2025 IEEE DELCON-International Conference on Recent Smart Technologies in Engineering for Sustainable Development* (pp. 1-5). IEEE.
- [4] Harun, N.Z., 2023. Distributed Denial of Service (DDoS) Detection Tool Using Artificial Neural Network (ANN) for Homelab. *Applied Information Technology And Computer Science*, 4(2), pp.139-158.
- [5] Christy, V.M., Srinivasan, R., Kousalya, E., Reena, P. and Fathima, M.B., 2025. Real-Time DDoS Attack Detection using Random Forest and Streamlit: A Machine Learning-Based Web Solution. *Central Asian Journal of Mathematical Theory and Computer Sciences*, 6(3), pp.361-375.
- [6] Sujatha, V. and Prabakeran, S., 2023, October. Lightweight DDoS Attack Detection and Mitigation in Software-Defined Networks Using Deep Learning. In *2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS)* (Vol. 1, pp. 1-8). IEEE.
- [7] Sadhwani, S., Manibalan, B., Muthalagu, R. and Pawar, P., 2023. A lightweight model for DDoS attack detection using machine learning techniques. *Applied Sciences*, 13(17), p.9937.
- [8] Madhumitha, M., Karthik, M., Dheeraj, A. and Dashvant, S., 2026, March. Enhancing Network Intrusion Detection with Random Forest and Federated Learning Algorithms. In *International Conference on Artificial Intelligence and Secure Data Analytics (ICAISDA 2025)* (pp. 1138-1151). Atlantis Press.

- [9] Ponnarasan, D.S.S., Manimegalai, R. and Mohan, V., 2025, August. Unsupervised Anomaly Detection for Network Intrusion Using Deep Autoencoders and Statistical Modeling. In *2025 International Conference on Next Generation Computing Systems (ICNGCS)* (pp. 1-10). IEEE.
- [10] Abulhassan, A., Rashid, I., Imam, M. and Binbeshr, F., 2025. DDoS attack detection in iot: A comparative resource and performance analysis of deep learning and machine learning models. *IEEE Access*.
- [11] Terawi, N., Ashqar, H.I., Darwish, O., Alsobeh, A., Zahariev, P. and Tashtoush, Y., 2025. Enhanced detection of intrusion detection system in cloud networks using time-aware and deep learning techniques. *Computers*, *14*(7), p.282.
- [12] Islam, U., Al-Atawi, A., Alwageed, H.S., Ahsan, M., Awwad, F.A. and Abonazel, M.R., 2023. Real-time detection schemes for memory DoS (M-DoS) attacks on cloud computing applications. *IEEE Access*, *11*, pp.74641-74656.
- [13] Sanjalawe, Y. and Althobaiti, T., 2023. DDoS Attack Detection in Cloud Computing Based on Ensemble Feature Selection and Deep Learning. *Computers, Materials & Continua*, *75*(2).
- [14] Abdullatif, A., Thilakarathne, N.N. and Aashiq, M., 2024. Machine Learning Enabled Novel Real-Time IoT Targeted DoS/DDoS Cyber Attack Detection System. *Computers, Materials & Continua*, *80*(3).
- [15] Gupta, B.B., Gaurav, A., Arya, V. and Chui, K.T., 2024, May. Efficient ddos attack detection through lightweight deep learning model in cloud computing environment. In *2024 IEEE 24th International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)* (pp. 208-212). IEEE.
- [16] Subbu, R. and Nikhil, P., 2025. *A Comparative Analysis of Hybrid Machine Learning Techniques for Network Intrusion Detection in Cloud Environments* (Doctoral dissertation, Dublin, National College of Ireland).
- [17] Yousuf, O. and Mir, R.N., 2022. DDoS attack detection in Internet of Things using recurrent neural network. *Computers and Electrical Engineering*, *101*, p.108034.