Archives available at journals.mriindia.com

International Journal on Advanced Computer Engineering and Communication Technology

ISSN: 2278-5140
Volume 14 Issue 01, 2025

A Result Paper on "SVM-RF Sentinel: Adaptive DDoS Detection"

Prof. K. N. Aaglave[1], Gaurav Manik Hegade[2], Aniket Shrikant Abhang[3], Kumar Popat Thorat[4], Prashant Hanumant Bagal[5]

[1]Guide, S. B. Patil College of Engineering
[2-5]Department of Computer Engineering, Savitribai Phule Pune University
kimaya.gaikwad08@gmail.com[1], gauravhegade01@gmail.com[2], abhanganiket1@gmail.com[3], kthoratdocs@gmail.com[4], bagalprashant0404@gmail.com[5]

Peer Review Information

Submission: 15 Feb 2025
Revision: 23 March 2025
Acceptance: 27 April 2025

Keywords

Real time Detection
Multiple Approach Algorithm Model
DDoS Detection

Abstract

DDoS (Distributed Denial of Service) attacks are one of the biggest threats to online services, such as websites, servers, and applications. These attacks flood systems with fake traffic, causing slowdowns, crashes, and major disruptions. This can lead to significant financial losses, damage to a company's reputation, and a poor user experience. Traditional methods to detect these attacks often struggle with the size, speed, and complexity of modern DDoS attacks, making it hard to protect systems effectively. This project develops a new DDoS detection system that uses advanced machine learning to overcome these limitations. The system employs two powerful algorithms: Support Vector Machine (SVM) and Random Forest. SVM is used for its strong ability to classify and identify patterns of malicious traffic, while Random Forest helps manage and analyze large datasets more effectively. By using these algorithms, the system enhances detection accuracy A key feature is its easy-to-use interface, which allows both technical and non-technical users to set up, monitor, and respond to security alerts without needing extensive training. This project offers a more accurate, faster, and secure method for detecting and managing DDoS attacks. By using advanced machine learning with enhanced security features, it provides a robust solution to one of the most challenging problems in network security today.

INTRODUCTION

In today's digital world, cybersecurity is very important for businesses and individuals. One major threat is Distributed Denial of Service (DDoS) attacks, which can make websites and online services unavailable by overwhelming them with too much traffic. These attacks can cause significant harm, including financial losses and damage to a company's reputation. As attackers become smarter, it is crucial to have effective ways to detect and stop these threats. The "SVM-RF Sentinel: Adaptive DDoS Detection" project aims to tackle this problem using machine learning. By using two powerful algorithms—Support Vector Machine (SVM) and Random Forest (RF)—we hope to create a strong system for detecting DDoS attacks in real time. SVM is great at handling complex data, while RF improves accuracy by combining the results of many decision trees. Together, these algorithms will help identify DDoS attacks quickly and accurately. This project is important because traditional methods of DDoS detection often rely on fixed rules that attackers can easily bypass. Our system will adapt and learn from new attack patterns, reducing false alarms and improving

detection rates. Additionally, we will create a user-friendly interface that allows network administrators to monitor traffic and manage the detection process with ease. In summary, the "SVM-RF Sentinel" project aims to enhance the ability to detect and respond to DDoS attacks, helping organizations protect their online services and maintain their digital presence in a constantly evolving cyber threat landscape.

LITERATURE SURVEY

[1] “Realtime Detection of DDoS Attacks using Ensemble Learning”

SN. Wilson, E. Brown, and Sharma (2023) explore the challenges associated with delayed responses in real-time DDoS attack detection systems. The paper highlights how ensemble learning techniques, specifically Boosting and Bagging, can significantly enhance detection accuracy while maintaining operational efficiency. It emphasizes the importance of balancing speed with resource optimization, making it a valuable contribution toward building responsive and cost-effective intrusion detection systems. This work supports the integration of ensemble-based solutions in real-time applications like the proposed SVM-RF Sentinel system.

[2] “Towards Real-Time DDoS Detection Using Big Data Analytics”

J. Green and H. Clark (2023) focus on the limitations of existing systems in handling large volumes of network traffic data in real time. Their approach leverages Big Data analytics integrated with machine learning models, aiming to provide scalable and adaptable detection mechanisms. By proposing enhancements in data processing pipelines and real-time integration, this paper bridges the gap between data volume and detection responsiveness. It lays the foundation for combining large-scale data handling with intelligent decision-making—something critical for modern systems.

[3] “Machine Learning for DDoS Attack Detection: A Review”

J. Smith and A. Lee (2022) provide a broad comparative review of supervised machine learning techniques in DDoS detection. The study identifies the core limitations of traditional methods, particularly their inability to adapt to rapidly evolving attack patterns. By advocating for hybrid models and better feature selection strategies, the authors promote a direction toward adaptive and intelligent detection systems. This paper validates the dual-approach design of the SVM-RF Sentinel, supporting the notion that flexibility in model choice increases resilience against evolving threats.

[4] “Enhanced Security Measures for DDoS Detection in IoT Networks”

P. Singh and M. Gupta (2022) investigate the vulnerabilities present in IoT environments, where resource constraints severely limit detection capabilities. The study demonstrates how lightweight machine learning algorithms and anomaly detection methods can be effectively deployed in such contexts. It advocates for models that are efficient, fast, and capable of detecting novel threats in low-power systems. This aligns with real-time detection priorities and extends the scope of DDoS protection to include emerging technologies like IoT.

[5] “Detection of DDoS Attacks using Machine Learning Techniques”

S. Kumar and P. R. Sharma (2021) tackle the challenge of evolving DDoS attacks that evade conventional detection systems. Using Random Forest and SVM classifiers, the authors show how a combined or selective approach can improve accuracy and detection speed. The research underscores the need for continuous model updates and feature refinement, reinforcing the adaptive essence of machine learning-based detection. This paper directly inspires the user-selective model approach in the SVM-RF Sentinel.

[6] “Evaluating the Performance of Machine Learning Models for Network Security”

D. Brown and M. Scott (2021) provide a real-world evaluation of machine learning models in the context of network security. The paper discusses the varying performance outcomes based on deployment conditions and dataset variability. It highlights the need for robustness and adaptability in model design, suggesting that no single algorithm consistently outperforms others across all conditions. This comparative insight justifies the flexibility offered by dual-model systems like SVM-RF Sentinel, where users can switch methods based on the context or data characteristics.

[7] “Hybrid Intrusion Detection System for DDoS Attacks”

SL. Zhang and X. Chen (2021) emphasize the limitations of single-method intrusion detection systems, proposing a hybrid model combining SVM and Random Forest. Their results indicate significant improvements in detection accuracy and adaptability. Although the study combines both models simultaneously, it supports the broader idea of ensemble strength, validating the effectiveness of offering multiple model paths—even when used independently as in the SVM-RF Sentinel.

[8] "Integrating Feature Selection Techniques in DDoS Attack Detection"
R. Lee and H. Park (2020) address the issues of overfitting and irrelevant features that can degrade detection performance. Their solution involves advanced feature selection and dimensionality reduction techniques to enhance model learning and generalization. The research encourages the integration of pre-processing stages to improve overall detection quality, which is a critical factor in the pre-classification stage of most ML-based intrusion detection systems.

[9] "An Effective Approach for DDoS Attack Detection Using Neural Networks"
M. Patel and R. Kumar (2020) propose the use of deep neural networks (DNNs) to reduce false positives and improve detection accuracy. Their results show how deeper architectures can identify complex traffic patterns, although they also highlight the computational cost involved. The findings suggest a trade-off between performance and efficiency, which justifies the selection of more lightweight models like SVM and Random Forest for real-time detection scenarios.

[10] "Advanced DDoS Detection Using Multilayer Perceptrons"
T. Martinez and C. Gonzalez (2019) focus on enhancing detection precision through Multi-Layer Perceptrons (MLPs). The paper demonstrates that MLPs are effective in capturing non-linear patterns, especially in complex DDoS scenarios. However, it also points to challenges in training and scalability, leading to a push for improving model efficiency. This research aligns with the trend of using simpler, yet powerful classifiers for real-time systems, as seen in the SVM-RF Sentinel model.

LIMITATIONS OF EXISTING WORK

- The accuracy of the detection model depends heavily on the quality and quantity of the training data.
- As the network grows and traffic increases, the model may need improvements to maintain consistent performance.
- The project is specifically designed to detect DDoS attacks and does not address other types of cyber threats.
- The system may struggle to detect entirely new or highly sophisticated DDoS attack patterns not represented in the training data.
- Real-time performance may be impacted by hardware limitations, especially in environments with high traffic volume.

PROBLEM STATEMENT
DDoS (Distributed Denial of Service) attacks overwhelm networks with excessive traffic, causing service disruptions and financial losses. Existing detection methods are often too slow, inaccurate, and lack extra security measures, making it difficult to protect networks effectively. There is a need for a faster, more accurate, and secure system to detect and manage these attacks in real time.

PROPOSED SYSTEM
The proposed system, SVM-RF Sentinel, is an intelligent and adaptive DDoS detection solution that leverages machine learning to identify malicious traffic patterns in real-time. The system processes incoming network traffic, extracts relevant features, and classifies the behaviour as either normal or DDoS attack. By providing a user-friendly GUI, it enables security personnel or administrators to monitor attack status and switch between detection algorithms based on performance or preference.

SYSTEM REQUIREMENTS
Operating System: Windows 10
IDE: Spyder(For coding)
Libraries: Pandas, Numpy
GUI: Anaconda Navigator
Programming Language: Python
Hardware:
RAM: 8GB
Hard Disk: 500GB
Processor: Intel i5 Processor
Speed: 2.4 GHz

METHODOLOGY

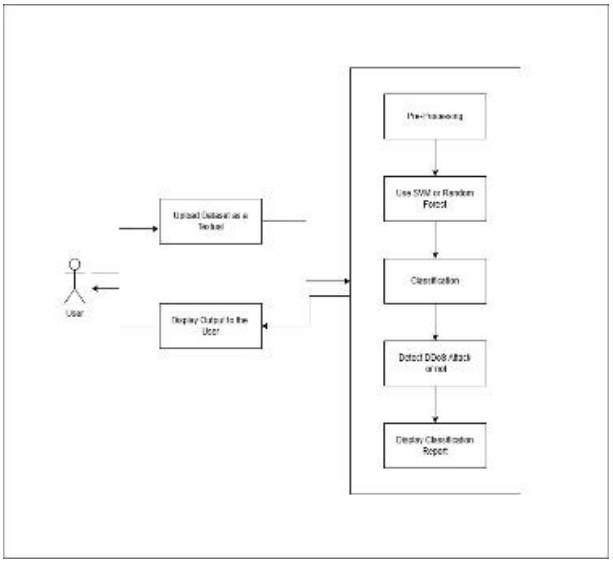


Fig 1. Architecture Diagram

1. User Interaction:-
User upload a dataset in **textual format** (likely containing network traffic data) into the system.

2. System Processing Flow:-

Once the dataset is uploaded,

- Pre-Processing: The uploaded data is cleaned, formatted, and prepared for analysis. This may involve feature extraction, normalization, or handling missing values.
- Use SVM or Random Forest: The user can choose between Support Vector Machine (SVM) or Random Forest (RF) for classification. Instead of combining both, your system allows selection of one model at a time, making it flexible.
- Classification: The selected model processes the dataset and classifies the data into normal or potential DDoS attack categories.
- Detect DDoS Attack or Not: Based on the classification results, the system determines whether a DDoS attack is present or not.
- Display Classification Report: The system generates a report summarizing the classification results, including metrics like accuracy, precision, recall, and F1-score.

3. **Output Display:-**The classification results are then displayed to the user in a readable format.

RESULTS / OUTPUTS

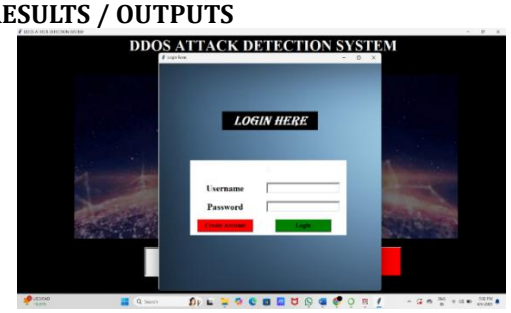


Fig 3. Login Page

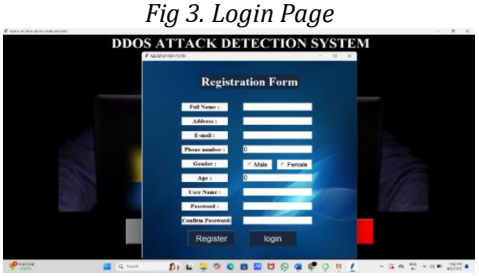


Fig 4. Registration Page

Fig 5. Home Page

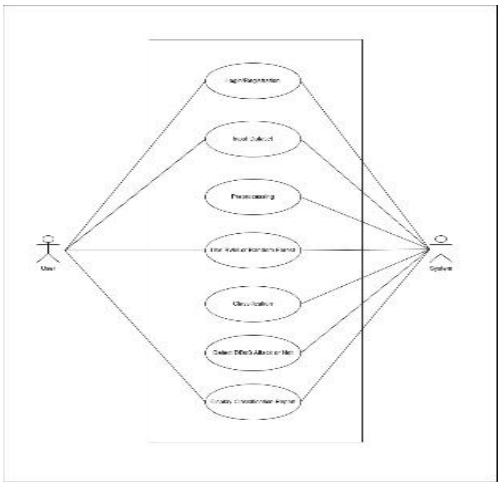


Fig 2. Use-case Diagram

RESULT DISCUSSION

The proposed system, SVM-RF Sentinel, was successfully detected DDoS attacks in real-time using both SVM and Random Forest algorithms. Random Forest achieved higher accuracy, while SVM performed better with smaller datasets. The GUI effectively displayed attack status, and users could flexibly switch between models. Overall, the system demonstrated reliable, efficient, and adaptable DDoS detection capabilities.

Fig 6. GUI

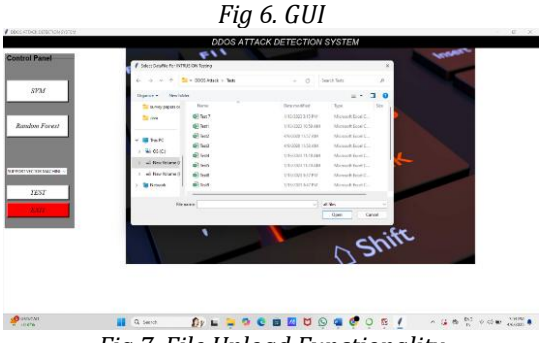
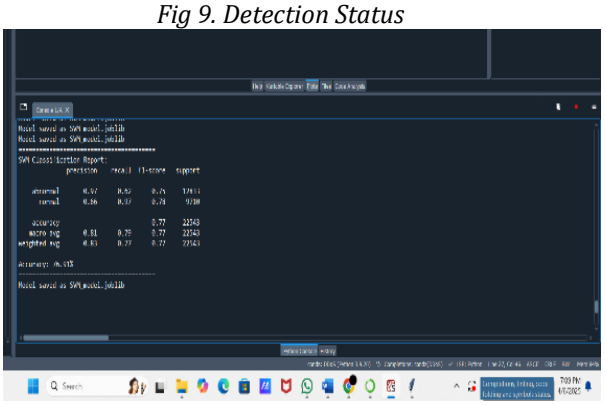


Fig 7. File Upload Functionality

Fig 8. Detection Status

Fig 10. Classification Report

Fig 9. Detection Status



CONCLUSION

In this paper, we presented the SVM-RF Sentinel: Adaptive DDoS Detection system, which leverages the strengths of Support Vector Machines (SVM) and Random Forest (RF) algorithms to provide an effective solution for identifying a Distributed Denial of Service (DDoS) attacks in real-time. By integrating these two robust machine learning techniques, our system enhances the accuracy of detect the attacks. The design of our project emphasizes not only high performance but also user-friendly Interface.

References

Vidyaev I G, Ivashutenko A S, Samburskaya M A. Smart Grid Concept As A Modern Technology For The Power Industry Development[C]// 2017:012173

Huang H B, Hong L, Chang-Yue Y U, et al. Analysis on Ukraine Power Grid Blackout and Its Enlightenment of ICS in China[J]. Standard Science, 2016.

Jianye Hao, Eunsuk Kang, Jun Sun, Zan Wang, "An Adaptive Markov Strategy for Defending Smart Grid False Data Injection from Malicious Attackers", IEEE Transactions on Smart Grid. Sept. 2016.

Jiaxuan Fei,Tao Zhang,Yuanyuan Ma,Cheng Zhou. A DDoS attack detection method for power grid industrial control system based on BF-DT-CUSUM algorithm[J]. Telecommunications Science.2015 (12).

Yanan Sun, Xiaohon Guan, Ting Liu, Yang Liu, "A cyber-physical monitoring system for attack detection in smart grid", Computer Communications Workshops (INFOCOM WKSHPS), 2013 IEEE Conference on, Turin, Italy, Dec. 2014.

Mina Rahbari and Mohammad Ali Jabreil Jamali, "Efficient Detection of Sybil Attack Based on Cryptography in VANET," IJNSA, Vol.3, No.6, November 2011.

Mohamed Salah Bouassida, Gilles Guette, Mohamed Shawky, and Bertrand Ducourthial, "Sybil Nodes Detection Based on Received Signal Strength Variations within VANET," International Journal of Network Security, Vol.9, No.1, PP.22-33, July 2009.

Mushtak Y. Gadkari, Nitin B. Sambre, "VANET: Routing Protocols, Security Issues and Simulation Tools," IOSR Journal of Computer Engineering, July-Aug. 2012.

Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, Aamir Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," Springer Science +Business Media, LLC 2010.

Wikipedia "Vehicular Ad-Hoc Network" http://en.wikipedia.org/wiki/Vehicularadhocnetwork this page was this page was last modified on 5 January 2013.