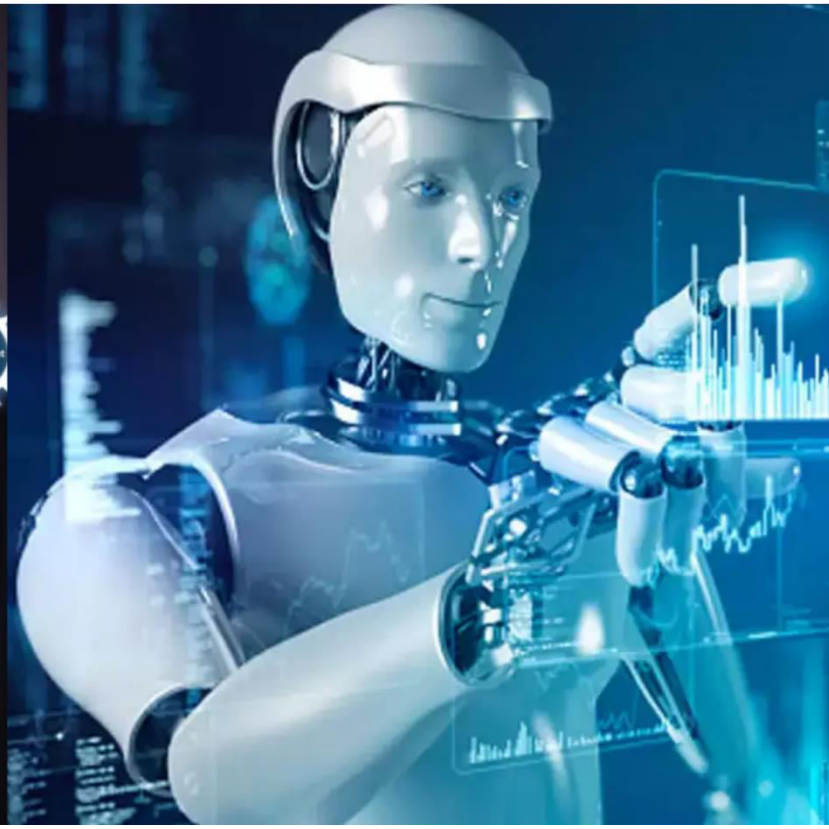
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 11, November 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411033|

AI-Powered Cyber Attack Detection & Mitigation Advisor

Prof. Dhage S.A.[1], Abhishek Wayal[2], Rahul Gadhave[3], Aniket Gadade[4]

Associate Professor, Department of Computer Engineering VACOE, Ahilyanagar, Maharashtra, India[1]

U.G. Student, Department of Computer Engineering, VACOE, Ahilyanagar, Maharashtra, India[2]

U.G. Student, Department of Computer Engineering, VACOE, Ahilyanagar, Maharashtra, India[3]

U.G. Student, Department of Computer Engineering, VACOE, Ahilyanagar, Maharashtra, India[4]

ABSTRACT: In an era of increasing digital connectivity, the need for advanced and proactive cyber threat detection has become critical. This project introduces CyberFedDefender, a system that leverages machine learning to address the inefficiencies of traditional, reactive security measures. The system is designed to build and deploy a robust classification model capable of distinguishing between normal network traffic and malicious activities, specifically focusing on DDoS and Ransomware attacks. By analyzing a rich dataset of network attributes, the project moves from data preprocessing to a fully containerized application. The core innovation is the integration of an AI Suggestion Module, which provides immediate, actionable mitigation advice tailored to the detected threat. The final system is delivered as a user-friendly web application with a React.js frontend and a Flask-based backend, aiming to significantly reduce reliance on manual monitoring and enhance an organization's security posture.

KEYWORDS: Cyber Attack Detection and Mitigation Advisor, Proactive.

I. INTRODUCTION

The landscape of cybersecurity is a constantly evolving digital battlefield where threats are becoming more sophisticated and relentless. Traditional security infrastructures, which often depend on manual analysis of network logs and alerts, are proving to be insufficient. These methods are inherently reactive, leading to significant delays between the time of an attack and its detection, which can result in substantial damage. The sheer volume of network traffic in modern enterprises makes manual monitoring for anomalies an impossible task, creating a critical vulnerability.

To address these challenges, this project proposes CyberFedDefender, an intelligent, AI-powered system designed to automate and enhance network security. By analyzing network traffic data, the system proactively detects and classifies cyber-attacks like DDoS and Ransomware. More importantly, it provides network administrators with intelligent, actionable recommendations for mitigation. The goal is to create a powerful decision-support tool that automates the identification of malicious activities, reduces response times, and minimizes the potential impact of cyber threats, thereby shifting the security paradigm from reactive to proactive.

II. EASE OF USE

This system is designed to simplify network security by replacing manual analysis with a user-friendly web application. It features an automated dashboard that displays attack predictions and, most importantly, provides direct, AI-generated mitigation suggestions.

This transforms the system into a powerful decision-support tool, reducing the complexity and response time for network administrators.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411033|

III. ABBREVIATIONS AND ACRONYMS

1. AI - Artificial Intelligence
2. ML - Machine Learning
3. DDoS - Distributed Denial of Service
4. IDS - Intrusion Detection System
5. IPS - Intrusion Prevention System
6. API - Application Programming Interface
7. RDP - Remote Desktop Protocol

IV. MODULES

• Data Preparation and Analysis Module: This initial module is responsible for ingesting the raw cyberdefender-dataset.csv file. It cleanses the data, handles inconsistencies, and performs exploratory data analysis (EDA) to understand the underlying patterns and features of the network traffic.
• Machine Learning Model Training Module: This module utilizes the prepared data to build and train the core classification model. It is here that the algorithm learns to accurately distinguish between normal network traffic and malicious patterns associated with DDoS and Ransomware attacks. The output of this module is the trained .pkl model file.
• Backend API Module: Developed using Python and Flask, this module serves as the brain of the application. It loads the trained ML model and exposes it through an API endpoint. When it receives data from the frontend, it processes the input, generates a prediction, and retrieves the appropriate mitigation advice.
• AI Suggestion Module: This is the project's core innovation. It consists of a knowledge base and logic that maps the model's prediction (e.g., "DDoS detected") to specific, actionable mitigation steps. Instead of generic advice, it provides context recommendations to help administrators respond effectively.
• Frontend User Interface: This module is the user-facing web dashboard built with React.js. It provides a simple interface for a security administrator to input network parameters, view the resulting threat classification, and read the AI-generated mitigation suggestions clearly.
• Deployment Module (Docker Container): To ensure portability and scalability, the entire backend application—including the Flask API and the trained model—is encapsulated within a Docker container. This allows the system to be deployed consistently and reliably in any environment.

V. TOOLS AND TECHNOLOGY

The development of CyberFedDefender relies on a modern, robust technology stack to ensure efficiency, scalability, and maintainability.
• Python with Flask: The backend of the application, including the machine learning model serving and the suggestion logic, is built using Python with the Flask micro-framework. Flask is used to create a RESTful API that the frontend consumes.
• Machine Learning Libraries: Core libraries such as Scikit-learn, Pandas, and NumPy are utilized for data preprocessing, exploratory data analysis (EDA), and the development and training of the classification model.
• React.js: The frontend user interface is developed as a dynamic and responsive application using React.js. It provides an intuitive dashboard for users to input data, view predictions, and receive mitigation suggestions.
• Docker: To ensure portability and ease of deployment, the entire backend application, including the trained model, is containerized using Docker. This allows the system to run consistently across different environments

VI. SYSTEM ANALYSIS AND INNOVATION

Limitations of Existing Systems

Current cybersecurity practices in many organizations rely on a combination of traditional Intrusion Detection/Prevention Systems (IDS/IPS) and human analysts. This approach has several inherent weaknesses:
• Manual and Slow: Security analysts must manually sift through countless alerts and logs to identify genuine threats, a process that is slow and inefficient.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411033|

• Prone to Human Error: The complexity and volume of data can lead to misinterpretation or missed threats.
• Reactive Nature: Response actions are typically initiated only after an alert has been analyzed, by which time damage may have already occurred.
• Not Scalable: As network traffic grows, a manual approach cannot scale effectively to provide comprehensive protection.

VII. PROPOSED SYSTEM AND INNOVATION

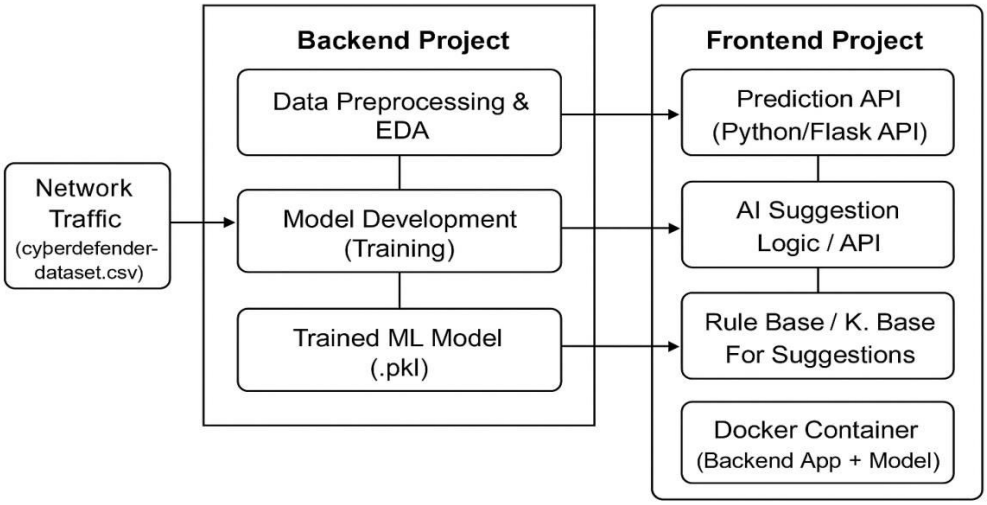


Fig: Proposed System Architecture

The CyberFedDefender system is designed to overcome these limitations through automation and artificial intelligence. The proposed system features an automated web dashboard that displays immediate predictions for submitted network parameters.
The key innovation of this project is the AI Suggestion Module. Unlike traditional systems that simply flag a potential threat, our system provides contextual and actionable intelligence. For a detected DDoS attack, it might suggest, "Implement rate limiting for source IP X," or for Ransomware, "Isolate affected server Y and check for recent RDP vulnerabilities". This transforms the system from a simple detection tool into a powerful decision-support advisor, significantly reducing the cognitive load on administrators and enabling a much faster, more effective response.

VIII. BACKGROUND REVIEW AND LITERATURE REVIEW

The application of Artificial Intelligence in cybersecurity is a rapidly growing field aimed at overcoming the limitations of conventional security tools. Traditional signature-based detection systems struggle to identify novel, or "zero-day," attacks, as they rely on known patterns. Machine Learning (ML), a subset of AI, offers a more dynamic approach by learning from data to identify patterns and anomalies that may indicate a threat.

Several studies have demonstrated the effectiveness of ML in intrusion detection. Supervised learning algorithms, such as Decision Trees, Support Vector Machines (SVM), and Neural Networks, have been successfully used to build classification models that can distinguish between benign and malicious network traffic with high accuracy. These models are trained on large, labelled datasets containing various network features like packet length, protocol, and flow duration.

In the context of specific threats, research has focused on anomaly detection for identifying DDoS attacks. These attacks are characterized by an overwhelming flood of traffic from multiple sources, and ML algorithms can be trained to

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411033|

recognize the shifts in network behavior that constitute such an attack. Similarly, for Ransomware, ML models can be designed to detect anomalous behaviors such as rapid, widespread file encryption, enabling detection before significant damage is done. Our project builds upon this existing body of research by not only detecting these threats but also bridging the gap between detection and response through an intelligent advisory component.

IX. APPLICATION OF CYBERFEDDEFENDER

The CyberFedDefender system is designed with several practical applications aimed at enhancing organizational cybersecurity. Its primary uses extend from direct threat identification to strategic security management.

• Automated Threat Detection and Classification

The system's core application is to automate the detection of malicious network activities. By analyzing network traffic attributes, it functions as an advanced security tool capable of identifying and classifying specific, high-impact cyber-attacks.

• DDoS Attack Identification: The model is trained to recognize traffic patterns indicative of a Distributed Denial of Service (DDoS) attack.

• Ransomware Detection: It can effectively distinguish network behaviors associated with Ransomware, allowing for early identification.

• Intelligent Decision Support for Security Personnel: A key innovation of the project is its application as a decision-support tool for network and security administrators. The system does not just alert users to a problem; it guides their response.

• Actionable Mitigation Advice: Upon detecting a threat, the AI Suggestion Module provides immediate, actionable mitigation steps tailored to the specific attack.

• Reduced Response Time: By offering direct recommendations, the system significantly reduces the cognitive load and analysis time for administrators, enabling a faster and more effective response.

X. FUTURE DIRECTIONS AND RESEARCH OPPOETUNITIES

While CyberFedDefender provides a robust foundation, there are several avenues for future enhancement to create an even more powerful security tool.

The immediate next step is to integrate the system with real-time stream processing frameworks like Apache Kafka. This would allow for continuous, live monitoring of network traffic rather than relying on static, user-submitted datasets. The suggestion module could be evolved from a rule-based system into an adaptive engine using concepts from Reinforcement Learning, allowing it to learn from the effectiveness of its past suggestions. Furthermore, incorporating unsupervised learning models would enable the detection of novel, zero-day attacks that the current model has not been trained on. For a more comprehensive security posture, the system could be integrated with external threat intelligence feeds to enrich the input data and improve detection accuracy. Finally, exploring secure integration with network hardware like firewalls could allow for the automated implementation of mitigation strategies, with human oversight.

XI. CONCLUSION

The CyberFedDefender project successfully demonstrates the significant potential of machine learning to revolutionize cyber security practices. By automating the complex task of network traffic analysis, our system provides an efficient, scalable, and proactive solution for identifying critical threats like DDoS and Ransomware. The integration of the AI Suggestion Module is a crucial innovation that elevates the system beyond simple threat detection, transforming it into an intelligent decision-support tool that empowers administrators to act swiftly and decisively. The modular, containerized architecture ensures that the system is robust, maintainable, and prepared for future enhancements. This work contributes to the development of more resilient digital environments by strengthening an organization's defensive posture against the ever-evolving landscape of cyber warfare.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411033|

REFERENCES

1. Mumtaz, G., Akram, S., Iqbal, M. W., Ashraf, M. U., Almarhabi, K. A., Alghamdi, A. M., & Bahaddad, A. A. (2023). Classification and Prediction of Significant Cyber Incidents (SCI) Using Data Mining and Machine Learning (DM-ML). IEEE Access, 11, 94486-94496.
2. Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.
3. Doshi, R., Apalkova, N., & Sakir, B. (2018). Machine Learning for DDoS Attack Detection: A Systematic Review. 2018 IEEE 12th International Conference on Application of Information and Communication Technologies (AICT), 1-6.
4. Scaife, N., Carter, H., & Traynor, P. (2016). CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS), 303-312.
5. Ahmad, I., Basheri, M., Iqbal, M. J., & Rahim, A. (2018). Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection. IEEE Access, 6, 33789-33795.
6. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. Proceedings of the 4th International Conference on Information Systems Security and Privacy, 108-116.
7. Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2017). Applying deep learning approaches for network traffic prediction. 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI) , 589-595.
8. Grinberg, Y. (2018). Flask Web Development: Developing Web Applications with Python. O'Reilly Media, Inc.
9. Kwon, D., Kim, H., Kim, J., Suh, S. C., Kim, I., & Kim, K. J. (2017). A survey of deep learning-based network anomaly detection. Cluster Computing, 22(1), 949-961.
10. Sahu, A. K., & Sharma, S. (2020). A comprehensive survey on machine learning based ransomware detection. 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), 725-731.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details