IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, December 2025
Impact Factor: 7.67

AI Enabled Threat Detection

Prof. Oruganti Kalpana[1], Pratyasha pradhan[2], Bhavana S[3], G G Sriya[4], Preethika M[5]
[12]Assistant Professor, CS&E Dept, Proudhadevaraya Institute of Technology, Hosapete, Karnataka, India
[345]Students, CS&E Dept, Proudhadevaraya Institute of Technology, Hosapete, Karnataka, India

Abstract: *This project presents an **AI Enabled Threat Detection System** designed to identify malicious network activities with improved accuracy and efficiency. Traditional security mechanisms rely on static rules and signatures, which are ineffective against modern and unknown cyber threats. The proposed system integrates machine learning techniques to analyze network traffic behavior and classify it as benign or malicious. The system uses the XGBoost algorithm for efficient threat classification and provides real-time detection through a simple web-based interface. This approach reduces false positives, improves detection speed, and enhances overall network security.*

Keywords: AI Enabled Threat Detection, Machine Learning, Intrusion Detection System, XGBoost, Cyber Security, Network Security

I. INTRODUCTION

With the rapid growth of internet-based services and connected devices, cyber threats have become more frequent and sophisticated. Conventional intrusion detection systems based on predefined signatures fail to detect zero-day attacks and evolving threat patterns. Machine learning techniques enable systems to learn from network behavior and identify anomalies automatically. AI-based threat detection improves accuracy, scalability, and real-time response, making it suitable for modern cybersecurity requirements.

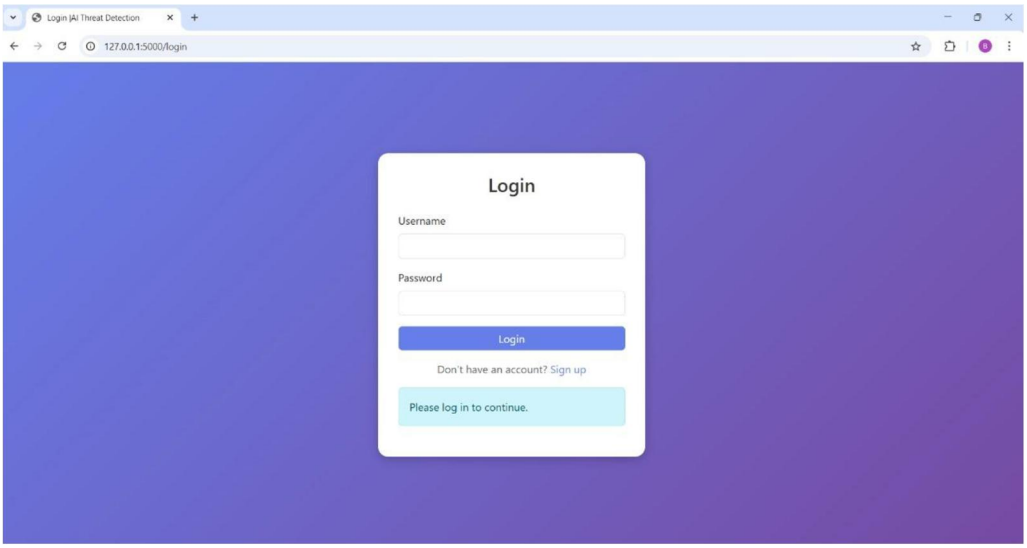
II. SYSTEM DESIGN

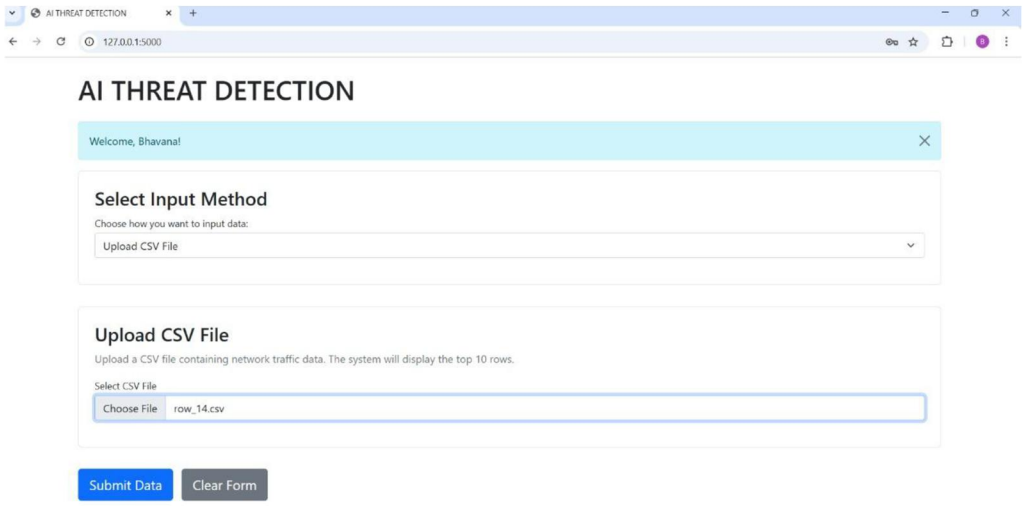
The proposed system follows a simple architecture consisting of a data processing module, a machine learning detection model, and a web-based user interface. Network traffic data is preprocessed and analyzed using the XGBoost algorithm to classify traffic into normal or attack categories. The trained model is integrated into a Flask-based web application that allows users to perform manual input detection or bulk CSV-based analysis. The system provides quick and reliable threat detection with minimal computational overhead.

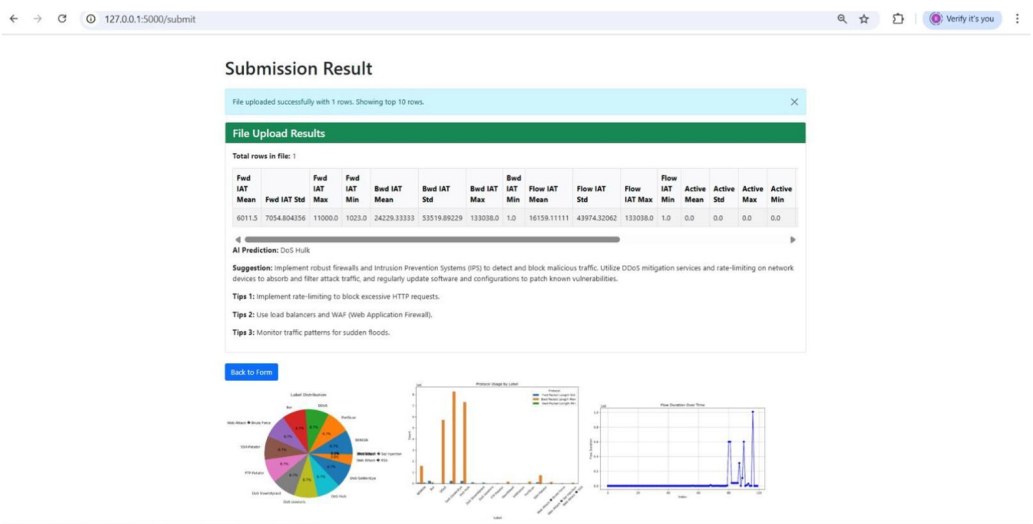
III. RESULTS AND DISCUSSION

The AI Enabled Threat Detection System successfully detects multiple types of network attacks such as DoS, DDoS, Port Scanning, Brute Force, and SQL Injection. The use of XGBoost improves classification accuracy while reducing false alarms. The web interface enables easy interaction and real-time prediction. Experimental results demonstrate that the system performs efficiently even on standard hardware, making it suitable for academic and small-scale deployment.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, December 2025
Impact Factor: 7.67







DOI: 10.48175/IJARSCT-30491

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, December 2025
Impact Factor: 7.67

IV. CONCLUSION

This project demonstrates the effective use of artificial intelligence in network security. By integrating machine learning with a lightweight web application, the system provides accurate and real-time threat detection. The AI Enabled Threat Detection System overcomes the limitations of traditional security approaches and offers a scalable and practical solution for modern cybersecurity challenges. The system can be further enhanced by incorporating real-time traffic capture and advanced learning models.

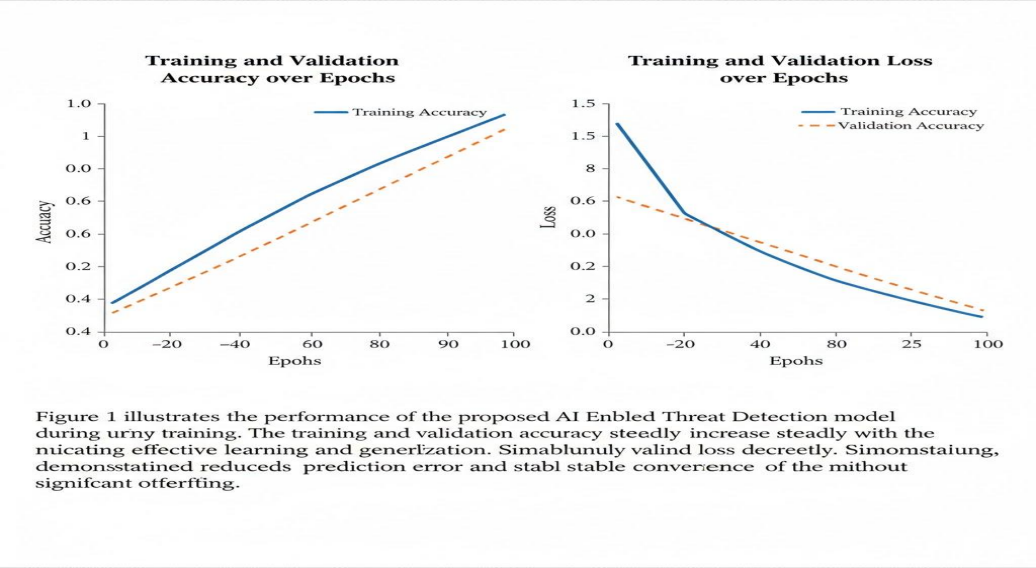


Figure 1 illustrates the performance of the proposed AI Enbled Threat Detection model during urny training. The training and validation accuracy steedly increase steadly with the nuicating effective learning and generlzation. Simablunuly valind loss decreetly. Simomstaiung, demonsstatined reduceds prediction error and stabl stable convenence of the mithout signifcant otferfting.

REFERENCES

[1]. Sharafaldin, A. Habibi Lashkari, and A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset," *CICIDS 2018*.
[2]. M. Tavallaee et al., "A Detailed Analysis of the KDD CUP 99 Dataset," IEEE, 2009.
[3]. C. Yin et al., "A Deep Learning Approach for Intrusion Detection," *IEEE Access*, 2017.
[4]. T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," *ACM SIGKDD*, 2016.