Detecting Anomalous Network Traffic Using AI

[1]G. Ramanaiah,[2]K. C. K. Ranga Pavan,[3]P. Krishna,[4]J. Bunny,[5]S. Shohel,[6]B. Vishnu Vardhan

[1]Assistant Professor, Dept of AI&ML, Dr.Samuel Gerorge Institute of Engineering & Technology, Darimadugu Village, Markapur, Prakasam, Idupur, Andhra Pradesh 523320.

[2,3,4,5,6]U. G Student, Dept of AI&ML, Dr.Samuel Gerorge Institute of Engineering & Technology, Darimadugu Village, Markapur, Prakasam, Idupur, Andhra Pradesh 523320.

ABSTRACT- ***The rapid expansion of network-based applications and internet services has significantly increased the risk of cyber-attacks such as denial-of-service attacks, probing, malware intrusions, and unauthorized access. Conventional intrusion detection systems rely on predefined rules and signatures, making them ineffective against novel and evolving attack patterns. To address these challenges, this project presents an Artificial Intelligence-based approach for detecting anomalous network traffic .The proposed system employs machine learning techniques to learn normal network behavior and identify deviations that indicate potential security threats. Network traffic data is collected from standard intrusion detection datasets and undergoes preprocessing, feature extraction, and normalization to improve detection efficiency***

Keywords: ***Network Security, Machine Learning, Random Forest, Cybersecurity, Feature Extraction***

INTRODUCTION

The rapid growth of network-based applications and internet services has revolutionized communication, commerce, and access to information, yet it has simultaneously increased the vulnerability of digital infrastructures to cyber threats. Modern networks are susceptible to a wide variety of attacks, including denial-of-service (DoS), distributed denial-of-service (DDoS), malware intrusions, phishing attacks, probing, and unauthorized access. Cyber-attacks have become more sophisticated and frequent due to the proliferation of interconnected devices, cloud computing, mobile platforms, and the Internet of Things (IoT). These attacks not only compromise sensitive information but also disrupt critical services, damage organizational reputation, and impose significant financial losses. Traditional intrusion detection systems (IDSs) rely on predefined rules and signature-based detection, which are effective against known threats but fail to identify novel and zero-day attacks. Signature-based systems

require constant updates to maintain accuracy, leading to delays in detecting emerging threats and leaving networks exposed during the update interval. Moreover, static rules cannot capture the dynamic and evolving patterns of modern cyber-attacks, particularly those that use polymorphic malware, stealthy behaviors, or multi-stage attack strategies.

As cyber threats become increasingly complex, the need for adaptive and intelligent detection mechanisms has grown significantly. Artificial intelligence (AI) and machine learning (ML) provide promising solutions to these challenges by enabling systems to learn patterns, identify anomalies, and adapt to new threats without explicit programming.

LITERATURE SURVEY

Several studies highlight that anomaly-based intrusion detection systems outperform traditional rule-based methods in detecting unknown attacks. Researchers have demonstrated that machine learning algorithms such as Random Forest, Support Vector Machine, and Neural Networks effectively analyze network traffic features. However, challenges such as high false-positive rates and scalability limitations still exist, emphasizing the need for improved AI-driven detection systems.

RELATED WORK

Previous research primarily focused on signature-based intrusion detection and statistical traffic analysis. Recent advancements incorporate machine learning models trained on benchmark datasets such as NSL-KDD and CICIDS. These models improve detection accuracy by identifying deviations from normal traffic behavior. Ensemble learning approaches, particularly Random Forest, have shown superior performance in handling complex network pattern.

EXISTING SYSTEM

Existing intrusion detection systems rely on rule-based and signature-based approaches to identify network attacks. These systems require frequent manual updates and fail to detect new or unknown threats. High false-positive rates and inefficiency in handling large-scale network data limit their effectiveness in real-time environments.

PROPOSED SYSTEM

The proposed system introduces an Artificial Intelligence (AI)-based approach to detect anomalous network traffic effectively. Unlike traditional rule-based security systems, the proposed model learns normal network behavior from historical traffic data
and identifies deviations that indicate

potential cyber-attacks. This intelligent system is capable of detecting both known and unknown attacks with higher accuracy.The system

collects network traffic data from benchmark datasets or live network sources and performs preprocessing operations such as data cleaning, normalization, and feature encoding.

Important network features are selected to reduce dimensionality and improve detection efficiency. Machine learning algorithms such as Random Forest, Support Vector Machine (SVM), and Isolation Forest are used to train the model. Once trained, the system classifies incoming network traffic as normal or anomalous in real

SYSTEM ARCHITECTURE

The system follows a three-tier architecture consisting of a presentation layer, application layer, and data layer.

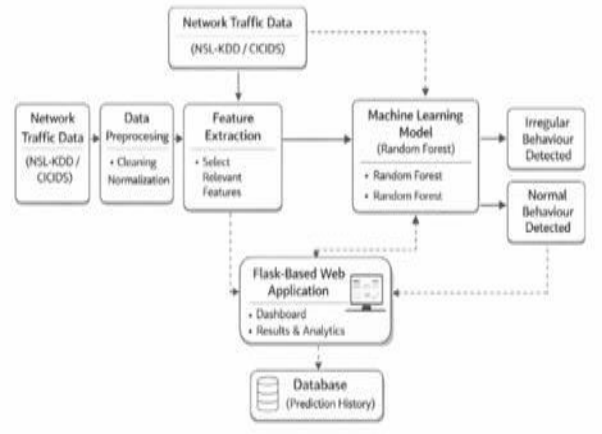

Fig.1 Architecture

METHODOLOGY DESCRIPTION

The methodology involves collecting network traffic data and extracting key features such as packet count, duration, protocol type, and error rates. These features are normalized and fed into machine learning models including Random Forest and Logistic Regression. The trained model predicts whether the network behaviour is normal or irregular. The prediction is processed by a Flask-based backend and displayed to the user via the web interface.

RESULTS AND DISCUSSION

User Registration Page: The registration page enables new users to create secure accounts by submitting basic credentials.

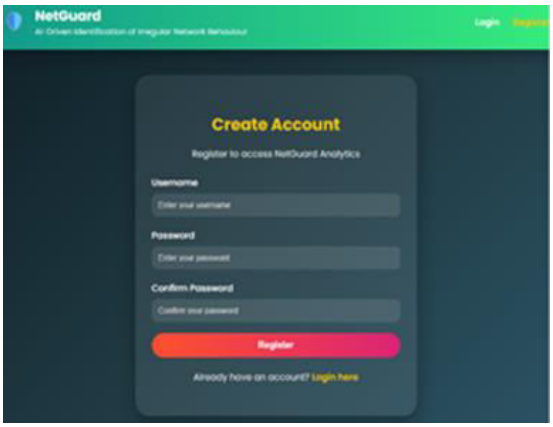

Fig.2 Register Page

User Login Page: The login module authenticates users before system access. This ensures secure entry and prevents unauthorized usage.

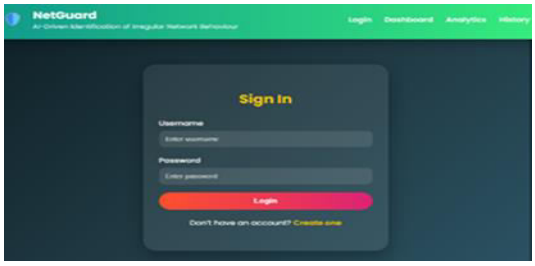

Fig.3 Login Page

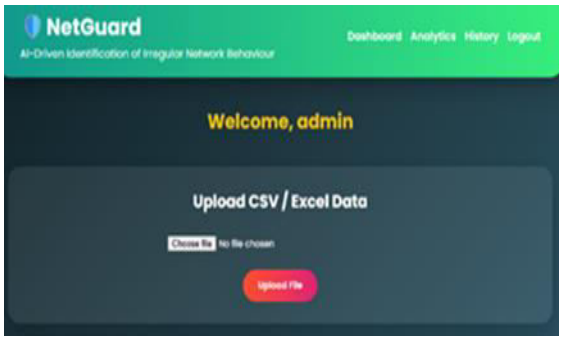

Fig.4 Dashboard

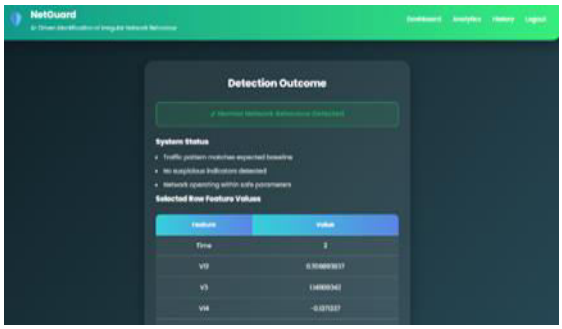

Fig.5 Normal Behaviour

Normal Network Behaviour Result: The system correctly identifies benign network traffic and displays a normal behavior result, confirming accurate learning of legitimate patterns.

CONCLUSION

This paper presented an AI-Driven Identification of Irregular Network Behaviour system that combines machine learning and web technologies to enhance network security. The proposed solution effectively detects anomalous activities, reduces false alarms, and supports scalable real-time monitoring. Future work includes integrating deep learning models, live packet capture, automated alert mechanisms, and advanced visualization dashboards to further strengthen network defense capabilities.

FUTURE SCOPE

Future enhancements include real-time packet capture, deep learning-based detection models, cloud deployment, automated alert systems, and integration with SIEM tools for enterprise-level security monitoring.

REFERENCES

[1] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, “A detailed analysis of the KDD CUP 99 data set,” Proc. IEEE Symp. Computational Intelligence for Security and Defense Applications, pp. 1–6, 2009.

[2] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “Toward generating a new intrusion detection dataset and intrusion traffic characterization,” Proc. ICISSP, pp. 108–116, 2018.

[3] V. Chandola, A. Banerjee, and V. Kumar, “Anomaly detection: A survey,”

ACM Computing Surveys, vol. 41, no. 3, pp. 1–58, 2009.

[4] R. Sommer and V. Paxson, “Outside the closed world: On using machine learning for network intrusion detection,” IEEE Symp. Security and Privacy, pp. 305–316, 2010.

[5] J. McHugh, “Testing intrusion detection systems: A critique of the 1998 and 1999 DARPA intrusion detection system evaluations,” ACM Trans. Information and System Security, vol. 3, no. 4, pp. 262–294, 2000.

[6] S. Axelsson, “Intrusion detection systems: A survey and taxonomy,” Technical Report, Chalmers University, 2000.

[7] T. Fawcett and F. Provost, “Adaptive fraud detection,” Data Mining and Knowledge Discovery, vol. 1, no. 3, pp. 291–316, 1997.

[8] L. Breiman, “Random forests,” Machine Learning, vol. 45, no. 1, pp. 5–32, 2001.

[9] M. L. Shyu et al., “A novel anomaly detection scheme based on principal component classifier,” Proc. IEEE ICDM, pp. 353–365, 2003.

[10] D. E. Denning, “An intrusion-detection model,” IEEE Trans. Software Engineering, vol. SE-13, no. 2, pp. 222–232, 1987.

[11] S. Mukkamala, A. H. Sung, and A. Abraham, “Intrusion detection using ensemble of soft computing paradigms,” Proc. IEEE Int. Conf. Fuzzy Systems, pp. 239–244, 2003.

[12] Y. Liao and V. R. Vemuri, “Use of k-nearest neighbor classifier for intrusion detection,” Computers & Security, vol. 21, no. 5, pp. 439–448, 2002.

[13] A. Patcha and J. Park, “An overview of anomaly detection techniques: Existing solutions and latest technological trends,” Computer Networks, vol. 51, no. 12, pp. 3448–3470, 2007.

[14] J. Zhang and M. Zulkernine, “Anomaly based network intrusion detection with unsupervised outlier detection,” Proc. IEEE ICC, pp. 2388–2393, 2006.

[15] C. C. Aggarwal, Outlier Analysis, 2nd ed., Springer, 2017.

[16] S. Revathi and A. Malathi, “A detailed analysis on NSL-KDD dataset using various machine learning techniques for intrusion detection,” Int. J. Engineering Research & Technology, vol. 2, no. 12, pp. 1848–1853, 2013.

[17] W. Stallings, Network Security Essentials: Applications and Standards, 6th ed., Pearson, 2017.

[18] K. Scarfone and P. Mell, “Guide to intrusion detection and prevention systems (IDPS),” NIST Special Publication 800-94, 2007.

[19] N. Moustafa and J. Slay, “UNSW-NB15: A comprehensive data set for network intrusion detection systems,” Military Communications and Information Systems Conference, pp. 1–6, 2015.

[20] A. A. Ghorbani, W. Lu, and M. Tavallaee, Network Intrusion Detection and Prevention, Springer, 2010.