International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X
www.ijdim.com
Original Research Paper

AI- Driven Identification of Irregular Network Behaviour

[1]Dr. A. Tirupatiah,[2]Shaik Zeenath Kousar,[3]Singothu Akhila,[4]Yakkati Devi Vineeth

[1]Associate Professor, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

[2,3,4]B. Tech Student, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

ABSTRACT

Ensuring network security has become a crucial concern due to the explosive proliferation of computer networks and internet-based services. Firewalls and signature-based intrusion detection systems are examples of traditional security measures that are frequently inadequate to identify changing and unidentified attack methods. The design and implementation of an AI-Driven Identification of Irregular Network Behaviour system, which uses machine learning techniques to identify anomalies in network data, are presented in this study. In order to categorise traffic as normal or irregular, the suggested system examines network flow characteristics taken from benchmark datasets like NSL-KDD and CICIDS. For precise detection, a Random Forest-based model is used; for real-time prediction and visualisation, the system is coupled with a Flask-based web application.

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

INTRODUCTION

Modern computer networks are increasingly vulnerable to cyber threats such as denial-of-service attacks, probing, and unauthorized access. Conventional (YS Krupamai, 2012/7)rules and signatures, making them ineffective against zero-day and adaptive attacks. Machine learning provides an intelligent solution by learning behavioral patterns from network traffic data. This project focuses on using AI-based techniques to automatically identify irregular network behaviour, enabling early threat detection and enhanced network security.

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.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X
www.ijdim.com
Original Research Paper

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 uses supervised machine learning algorithms to intelligently identify irregular network behaviour. Network traffic data is collected and preprocessed to extract relevant features. A trained classification model analyzes these features and classifies traffic as normal or irregular. The system is integrated with a web-based interface to provide real-time predictions, analytics, and historical monitoring, improving detection accuracy and scalability.

SYSTEM ARCHITECTURE

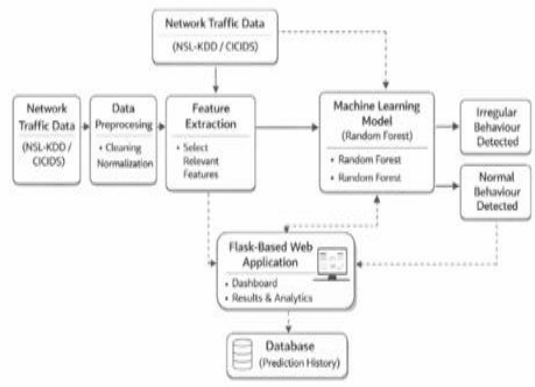

Fig 1: Architecture

The system follows a three-tier architecture consisting of a presentation layer, application layer, and data layer. Network traffic data is preprocessed and passed to the machine learning model for classification. Prediction results are stored in the database and displayed through a web-based dashboard for monitoring and analysis.

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.

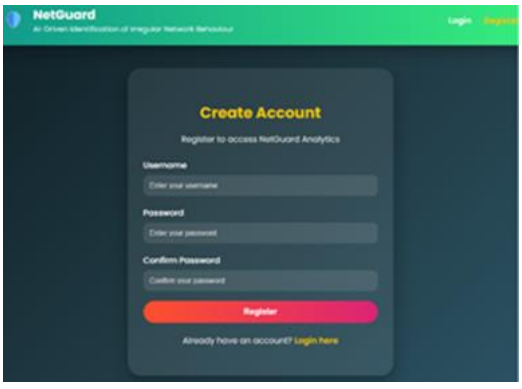

Fig 2: Register Page

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

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X
www.ijdim.com
Original Research Paper

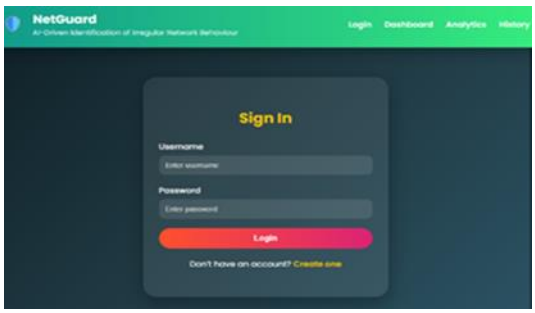

Fig.3 Login Page

Dashboard: This provides a centralized interface for uploading data, viewing predictions, and accessing analytics and history features.

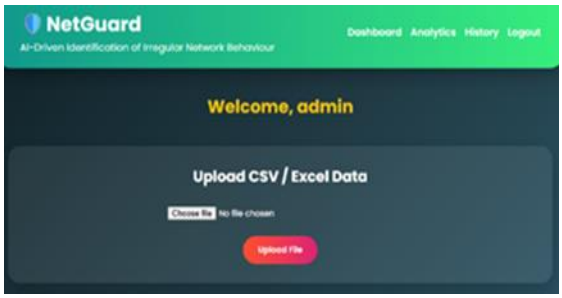

Fig.4 Dashboard

Processing: Uploaded network traffic data is preprocessed and forwarded to the trained machine learning model for classification.

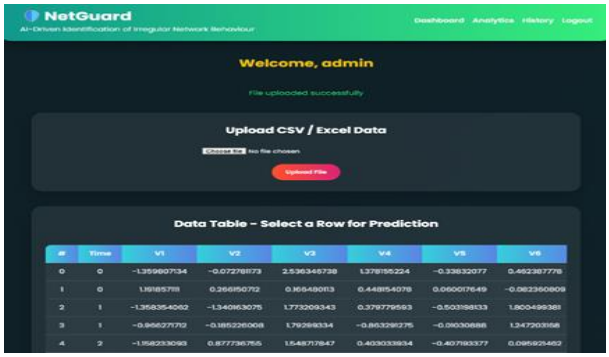

Fig.5 Dataset Uploading and Processing

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

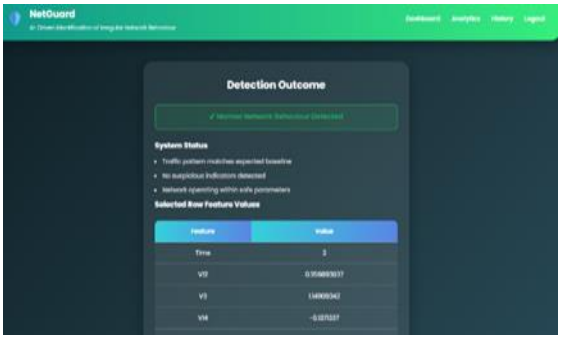

Fig.6 Normal Behaviour

Irregular Network Behaviour Result: An irregular behaviour result indicates detected anomalies or potential attacks, demonstrating effective intrusion detection.

Fig.7 Irregular Network Behaviour

Analytics Page: The analytics page visualizes detection results, helping administrators analyze network behaviour trends efficiently.

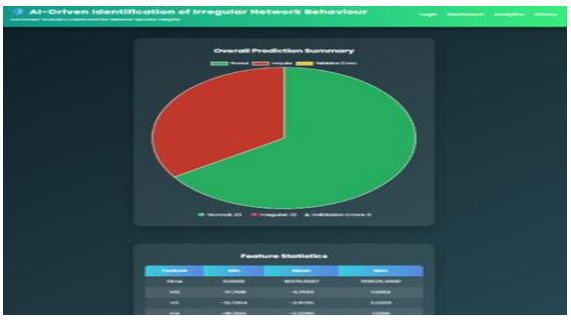

Fig.8 Analytics Page

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X
www.ijdim.com
Original Research Paper

Prediction History Page: The history page maintains past predictions with timestamps, supporting monitoring and audit analysis.

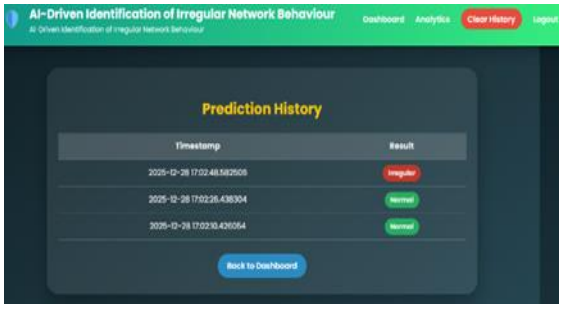

Fig.9 History Page

IX. 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.

X. 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.

XI. REFERENCES:

[1] Kesavulu, O. S. C., & Harini, P. (2013). Enhanced packet delivery techniques using crypto-logic riddle on jamming attacks for wireless communication medium. *Int. J. Latest Trends Eng. Technol*, *2*(4), 469-478.

[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.