AI Based Cyber Threat Prediction

Mrs.P.Uma Maheswari[1], Lekhashreel[2], Mahalakshmi S[3], Sreenithi V[4]
[1, 2, 3, 4] Dept of Computer Science and Business Systems
[1, 2, 3, 4] K. Ramakrishnan College Of Engineering, Trichy, India

Abstract- *The AI-Based Cyber Threat Prediction System improves cybersecurity using Artificial Intelligence, Machine Learning, and Deep Learning techniques. The system continuously monitors network traffic, system logs, and user activities to identify suspicious behavior and predict cyber threats in real time. CNN, RNN, and LSTM models are used for anomaly detection and threat prediction with improved accuracy.*

Keywords: Artificial Intelligence, Cybersecurity, Deep Learning, LSTM, Threat Prediction.

I. INTRODUCTION

BehaveGuard Cybersecurity has become a major concern due to the increasing use of internet services, cloud computing, IoT devices, and online transactions. Traditional security systems are ineffective against unknown and zero-day attacks. The proposed AI-Based Cyber Threat Prediction System uses intelligent algorithms to analyze network activities and predict cyber threats before they cause damage.

II. LITERATURE SURVEY

Researchers have explored Artificial Intelligence and Machine Learning techniques for intrusion detection and cyber threat prediction. Deep Learning models such as CNN and LSTM provide improved scalability, better accuracy, and faster response compared to traditional methods.

III. EXISTING SYSTEM

Traditional systems rely on firewalls, antivirus software, and signature-based intrusion detection systems. These methods are effective only for known attacks and suffer from high false positives and limited scalability.

IV. PROPOSED SYSTEM

The proposed system integrates Machine Learning and Deep Learning models to monitor network traffic and detect malicious activities. CNN, RNN, and LSTM algorithms are used for feature extraction, sequential analysis, and long-term dependency analysis.

V. METHODOLOGY

The methodology includes data collection, preprocessing, feature extraction, model training, anomaly detection, and alert generation. The system continuously updates using new datasets to improve prediction accuracy.

VI. SYSTEM ARCHITECTURE

The architecture consists of Presentation Layer, Business Logic Layer, and Data Layer. HTML, CSS, and JavaScript are used for frontend development, while Python and Flask are used for backend processing.

VII. MODULE IMPLEMENTATION

Modules include User Authentication, Dashboard, Data Monitoring, Prediction, Incident Response, and Security Assessment modules for intelligent cybersecurity management.

VIII. SYSTEM REQUIREMENTS

Hardware requirements include Intel Core i5 processor, 16 GB RAM, and SSD storage. Software requirements include Python, Flask, MySQL, TensorFlow, Keras, and Scikit-learn.

IX. SYSTEM TESTING AND RESULTS

The system successfully performed functionality, performance, and usability testing. Results demonstrated high prediction accuracy, fast response time, and improved threat detection capabilities.

X. CONCLUSION

The AI-Based Cyber Threat Prediction System provides an intelligent and scalable solution for modern cybersecurity challenges. The use of AI and Deep Learning technologies enables efficient detection of known and unknown cyber-attacks.

REFERENCES

[1] Husák, M., Komárková, J., Bou-Harb, E., & Čeleda, P. Survey of Attack Projection, Prediction, and Forecasting in Cyber Security.
[2] Sarker, I. H. CyberLearning: Machine Learning-Based Security Modeling for Cyber-Attack Detection.
[3] Nguyen, T. T., et al. Deep Learning for Cyberattack Detection in Mobile Cloud Computing.
[4] Zhang, Y., et al. Genetic Algorithm-Based Deep Belief Network for Cyber Attack Prediction.
[5] Silva, S., et al. Distributed Denial of Service Attack Prediction: Challenges and Opportunities.