AI-BASED CYBER THREAT DETECTION AND PREVENTION PLATFORM

[1]Dr. Y. Chitti Babu, [2]G. Bhargavi, [3]B. Lakshmi, [4]CH. Sai Lakshmi

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

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

ABSTRACT- ***Ai-Based Cyber Threat Detection And Prevention Platform is an intelligent cybersecurity system developed to detect and prevent cyber threats in computer networks using Artificial Intelligence (AI) and Machine Learning (ML). With the rapid growth of internet services, cloud computing, and digital communication, cyber attacks such as malware, phishing, ransomware, and network intrusions have increased significantly, making network security a major challenge for organizations and individuals.Traditional cybersecurity systems mainly depend on signature-based detection methods, firewalls, and antivirus software. These systems are effective only against known attacks and often fail to detect new or unknown threats, resulting in delayed detection, high false alarm rates, unauthorized access, and data breaches. To overcome these limitations, the proposed system uses Machine Learning to analyze network traffic and identify suspicious activities automatically.The proposed platform is developed using Python, Flask, Scikit-learn, Pandas, NumPy, and HTML, CSS, and Bootstrap for the web interface. The system is trained using the NSL-KDD dataset, and the Random Forest Machine Learning algorithm is used to classify network traffic as Normal or Anomalous with high accuracy. The platform also provides suitable prevention recommendations for detected threats, enabling users to take immediate security measures.***

Keywords: ***Artificial Intelligence, Machine Learning, Cybersecurity, Intrusion Detection System (IDS), NSL-KDD Dataset, Network Security, Threat Detection, Cyber Attack Prevention.***

INTRODUCTION

Cybersecurity is the practice of protecting computer systems, networks, and digital information from cyber attacks and

unauthorized access. With the rapid growth of the internet, cloud computing, online banking, e-commerce, and connected devices, the number of cyber threats has increased significantly. Attacks such as malware, phishing, ransomware, denial-of-service (DoS), and network intrusions can cause data breaches, financial losses, and disruption of services. Traditional security systems mainly depend on signature-based detection methods, which are effective only for known attacks and cannot identify new or evolving cyber threats efficiently.

To overcome these limitations, the uses Artificial Intelligence (AI) and Machine Learning (ML) to detect malicious activities automatically. The proposed system is developed using Python, Flask, Scikit-learn, Pandas, NumPy, HTML, CSS, and Bootstrap. It is trained using the NSL-KDD dataset, and the Random Forest algorithm is used to classify network traffic as Normal or Anomalous. The platform also provides suitable prevention recommendations for detected threats, helping users respond quickly to cyber attacks.

The developed web application allows users to upload datasets, train the Machine Learning model, perform cyber threat prediction, and view the results through a simple interface. This project provides an efficient, accurate, and reliable solution for improving network security and protecting modern digital systems from cyber threats.

RELATED WORK

Cyber threat detection is an important area of cybersecurity that focuses on identifying and preventing malicious activities in computer networks. With the rapid growth of internet services, cloud computing, and online applications, cyber attacks have become more frequent and sophisticated. Traditional cybersecurity systems mainly use signature-based detection methods, firewalls, and antivirus software to detect known attacks. However, these methods are not effective in identifying new and unknown threats, which has encouraged researchers to develop intelligent cyber threat detection systems using Artificial Intelligence (AI) and Machine Learning (ML).

Several research studies have applied Machine Learning algorithms such as Decision Tree, Random Forest, Support Vector Machine (SVM), K-Nearest Neighbors (KNN), and Naïve Bayes for intrusion detection. Researchers have also used benchmark datasets such as NSL-KDD to train and evaluate these models. These approaches have shown better accuracy, faster threat detection, and lower false alarm rates compared to traditional security methods. Some studies have also

explored Deep Learning techniques to improve intrusion detection performance.

The proposed is based on these research developments. It uses the NSL-KDD dataset and the Random Forest Machine Learning algorithm to classify network traffic as Normal or Anomalous. The system also provides prevention recommendations through a simple web-based interface, improving network security and helping users respond quickly to cyber threats.

LITERATURE SURVEY

Artificial Intelligence (AI) and Machine Learning (ML) have become important technologies in the field of cybersecurity. Many researchers have developed intelligent systems to detect cyber threats by analyzing network traffic and identifying suspicious activities. Unlike traditional security systems that depend on predefined signatures, AI-based systems can learn from previous data and detect both known and unknown attacks. This improves the efficiency and reliability of cyber threat detection while reducing the chances of security breaches.

Several studies have shown that Machine Learning algorithms such as Decision Tree, Random Forest, Support Vector Machine (SVM), and Naïve Bayes provide high accuracy in classifying network traffic as normal or malicious. Researchers have also used benchmark datasets like NSL-KDD to train and evaluate intrusion detection models. These intelligent systems help reduce false alarms, improve detection speed, and support real-time monitoring of network activities. The use of AI also enables automatic analysis of large amounts of network data, making cybersecurity systems more efficient and scalable.

The reviewed studies indicate that AI-based cyber threat detection systems offer better performance than traditional security methods. They help organizations identify attacks at an early stage, protect sensitive information, and minimize the impact of cyber threats. Based on these findings, the proposed uses Machine Learning to classify network traffic as Normal or Anomalous and provides appropriate prevention recommendations, ensuring improved network security and reliable protection against cyber-attacks.

EXISTING METHOD

Traditional cyber threat detection systems mainly rely on signature-based Intrusion Detection Systems (IDS), firewalls, and antivirus software to identify malicious activities. These systems compare network traffic with a database of known attack signatures to detect cyber threats. Although they provide effective protection against

previously identified attacks, they are unable to detect new or unknown threats such as zero-day attacks, ransomware, and advanced persistent threats. As the number of cyber attacks continues to increase, signature-based systems require frequent updates to their signature database, making them less effective against evolving attack patterns.

Many existing cybersecurity solutions also generate a high number of false alarms, making it difficult for network administrators to identify real threats. In addition, they do not analyze network traffic intelligently and cannot learn from previous attack patterns. This results in delayed threat detection and increases the risk of data breaches and unauthorized access. Most traditional systems also lack automated prevention mechanisms and require manual monitoring and response by security professionals.

Due to these limitations, existing cybersecurity methods are not sufficient to provide real-time and intelligent protection against modern cyber attacks. These drawbacks highlight the need for that can automatically analyze network traffic, accurately detect malicious activities, and provide suitable prevention recommendations.

PROPOSED METHOD

The proposed system is designed to overcome the limitations of traditional signature-based cybersecurity systems by using Artificial Intelligence (AI) and Machine Learning (ML). Unlike existing methods that detect only known attacks, the proposed system can identify both known and unknown cyber threats by analyzing network traffic patterns. The system is trained using the NSL-KDD dataset, which contains various types of normal and malicious network traffic records. During the training process, the Machine Learning model learns the characteristics of different cyber attacks and improves its detection accuracy.

When new network traffic is received, the trained model analyzes the data and classifies it as either Normal or Anomalous. If a malicious activity is detected, the system immediately provides suitable prevention recommendations to help users or network administrators take appropriate security measures. This intelligent approach reduces false alarms, improves detection speed, and minimizes the risk of data breaches and unauthorized access.

Compared to traditional security systems, the proposed platform provides higher accuracy, faster threat detection, and better network protection with minimal human intervention. The web-based application also allows users to upload datasets, train

the model, predict cyber threats, and view results through a simple interface. Therefore, the proposed system offers an efficient, reliable, and cost-effective solution for modern cyber threat detection and prevention.

SYSTEM ARCHITECTURE

The designed to detect and prevent cyber threats using Artificial Intelligence (AI) and Machine Learning (ML). The system begins with the user logging into the web application and uploading the NSL-KDD training and testing datasets. The uploaded data is sent to the preprocessing module, where missing values are handled, duplicate records are removed, and categorical data is converted into numerical form for efficient processing. The preprocessed data is then used to train the Machine Learning model, which learns the patterns of both normal and malicious network traffic.

After training, the model is saved and used for threat prediction. When a new dataset or network traffic data is uploaded, the system analyzes it using the trained model and classifies each record as either Normal or Anomalous. If a cyber threat is detected, the platform immediately provides suitable prevention recommendations to reduce security risks. Finally, the prediction results and prevention measures are displayed through a user-friendly web interface. This architecture improves detection accuracy, minimizes manual effort, enables faster decision-making, and provides an efficient solution for securing computer networks against modern cyber threats.

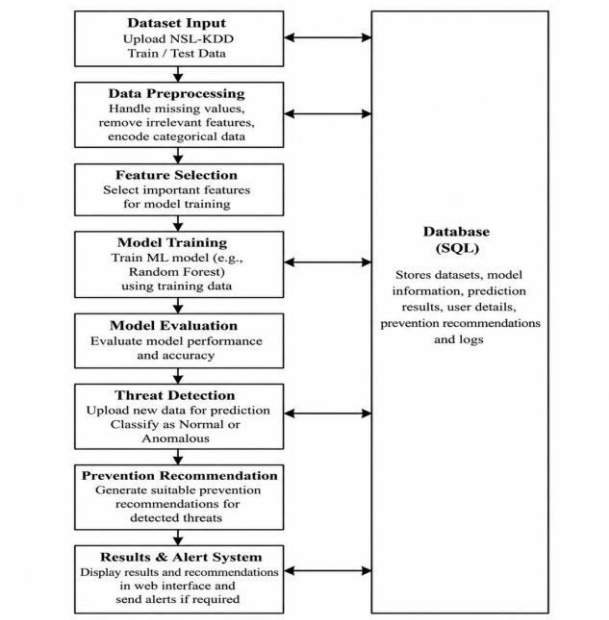

Fig 1: System Architecture

METHODOLOGY DESCRIPTION

1. Dataset Input

The proposed system starts by allowing the user to upload the **NSL-KDD** training and testing datasets through the web application. The uploaded dataset contains both normal and malicious network traffic records. These records are used to train and test the Machine Learning model so that it can accurately identify cyber threats and improve the overall security of computer networks.

2. Data Preprocessing

After uploading the dataset, the preprocessing module prepares the data for Machine Learning. It removes duplicate records, handles missing values, converts categorical attributes into numerical values, and normalizes the data. This process improves data quality, reduces errors, and increases the performance and accuracy of the cyber threat detection model.

3. Model Training

The preprocessed dataset is used to train the Machine Learning model. During training, the model learns the characteristics of both normal and malicious network traffic. The trained model identifies different attack patterns and is then saved for future predictions. This step enables the system to detect cyber threats efficiently with improved accuracy.

4. Cyber Threat Detection

Once the model is trained, the user can upload new network traffic data for analysis. The trained Machine Learning model examines each record and classifies it as **Normal** or **Anomalous** based on learned patterns. This process helps detect cyber attacks quickly, improves network monitoring, and reduces the possibility of security breaches.

5. Prevention Recommendation

If the system detects any malicious activity, it automatically generates suitable prevention recommendations to reduce security risks. The prediction results and recommended actions are displayed through the web interface, enabling users and network administrators to take immediate preventive measures. This improves network security and helps protect sensitive information from cyber-attacks.

RESULTS AND DECISION

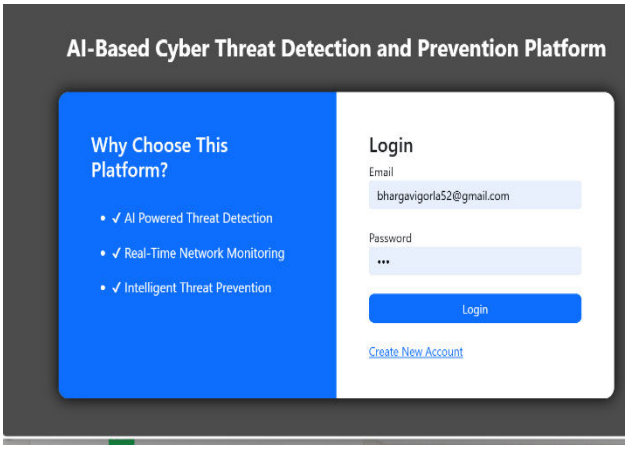

Fig 2: Login Page

The Login page allows registered users to securely access the AI-Based Cyber Threat Detection and Prevention Platform by entering their email and password. It also provides an option for new users to create an account.

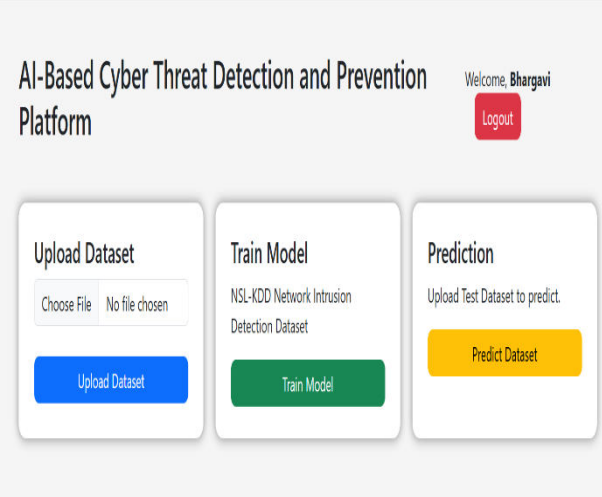

Fig 3: Dashboard

The Dashboard is the main interface of the application where users can upload the dataset, train the Machine Learning model, and perform cyber threat prediction. It provides easy access to all major functions of the system.

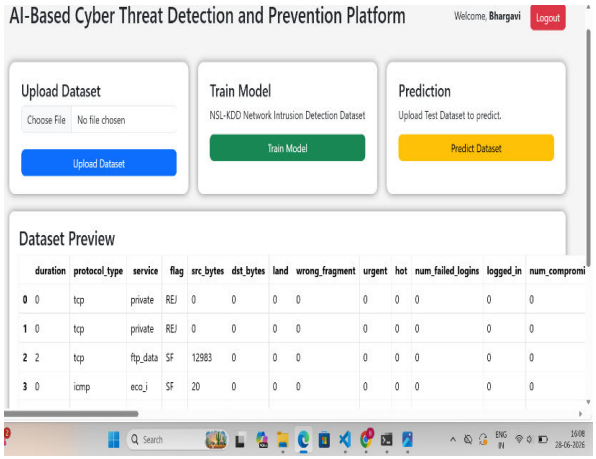

Fig 4: Dataset Upload

This page displays the uploaded NSL-KDD dataset in a tabular format. It allows users to verify that the dataset has been successfully uploaded before training the Machine Learning model.

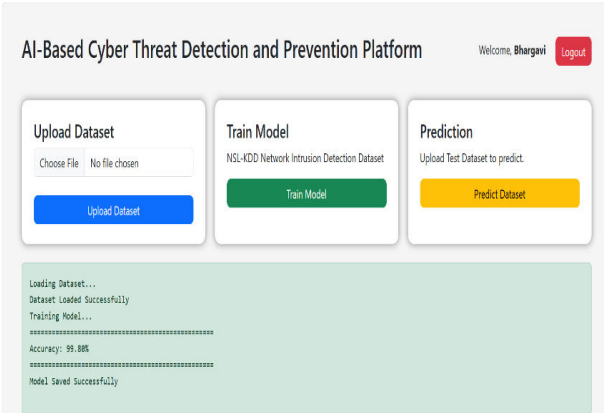

Fig 5: Model Training

The Model Training page trains the Machine Learning model using the uploaded NSL-KDD dataset. After successful training, it displays the model accuracy and confirms that the trained model has been saved.

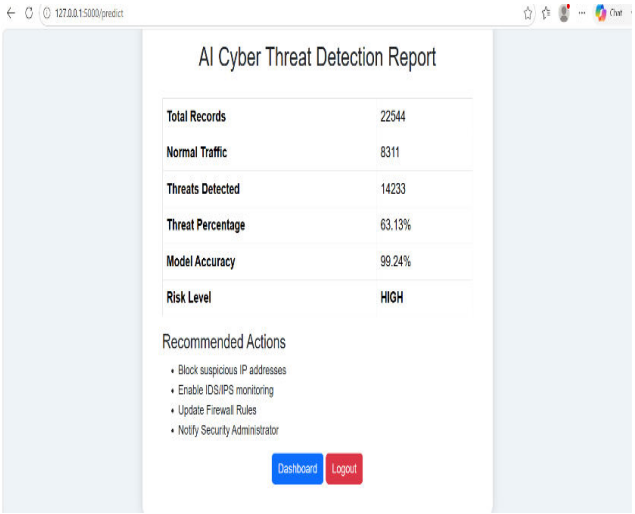

Fig 6: Prediction Result

The Prediction Result page displays the cyber threat detection report, including total records, normal traffic, detected threats, threat percentage, model accuracy, risk level, and recommended prevention actions for improving network security.

CONCLUSION

It provides an effective solution for identifying and preventing cyber-attacks using Artificial Intelligence and Machine Learning. The system uses the NSL-KDD dataset to train a Machine Learning model that accurately classifies network traffic as Normal or Anomalous. It enables users to upload datasets, train the model, perform predictions, and view prevention recommendations through a simple web interface. Compared to traditional security methods, the proposed system offers higher detection accuracy, faster threat identification, and reduced manual effort. Overall, this platform improves network security, protects sensitive information, and provides a reliable, efficient, and cost-effective solution for modern cyber threat detection and prevention.

FUTURE SCOPE

It can be enhanced by integrating real-time network monitoring to detect cyber attacks instantly. Future versions can use advanced Deep Learning algorithms to improve detection accuracy for unknown and zero-day attacks. The platform can also be connected with cloud-based threat intelligence to receive updated information about emerging cyber threats. Automated response mechanisms, such as blocking malicious IP addresses and isolating infected systems, can further strengthen network security. Integration with IoT devices and enterprise networks will make the platform more scalable, reliable, and suitable for protecting modern digital environments.

REFERENCES

[1] P. Harini, “Sms based wireless e-notice board,” *International Journal of Emerging Technology and Advanced Engineering,* vol. 3, no. 3, pp. 181-185, 2013.

[2] P. Harini, “Enhanced packet delivery techniques using crypto-logic riddle on jamming attacks for wireless communication medium,” *Int. J. Latest Trends Eng. Technol,* vol. 2, no. 4, pp. 469-478, 2013.

[3] P. Harini, “[Retracted] Machine Learning Algorithms Are Applied in Nanomaterial Properties for Nanosecurity,” *Journal of Nanomaterials,* vol. 2022, no. 1, p. 5450826, 2022.

[4] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.

[5] C. M. Bishop, *Pattern Recognition and Machine Learning*. New York, NY, USA: Springer, 2006.

[6] T. M. Mitchell, *Machine Learning*. New York, NY, USA: McGraw-Hill, 1997.

[7] F. Chollet, *Deep Learning with Python*, 2nd ed. Shelter Island, NY, USA: Manning Publications, 2021.

[8] S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed. Hoboken, NJ, USA: Pearson, 2021.

[9] A. Géron, *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow*, 3rd ed. Sebastopol, CA, USA: O'Reilly Media, 2022.

[10] Python Software Foundation, *Python Documentation*, Python.org, 2024.

[11] Scikit-learn Developers, *Scikit-learn: Machine Learning in Python Documentation*, Scikit-learn.org, 2024.

[12] Flask Development Team, *Flask Documentation*, Pallets Projects, 2024.

[13] P. Harrington, *Machine Learning in Action*. Shelter Island, NY, USA: Manning Publications, 2012.

[14] Open Web Application Security Project (OWASP), *OWASP Top 10: Web Application Security Risks*, OWASP Foundation, 2024.

[15] National Institute of Standards and Technology (NIST), *Cybersecurity Framework (CSF) 2.0*, Gaithersburg, MD, USA: NIST, 2024.