Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 4, No.2, April : 2025

AI BASED CYBERSECURITY THREAT DETECTION

N. Jaya Sree, CH. Devi Sri Harshitha, K. Eswar, M. Gowardhan Durga, Students, Department of Computer Science and Engineering SRK Institute of Technology, NTR, Andhra Pradesh, India
Dr. P. Srinivas Kumar, Associate Professor, Department of Computer Science and Engineering, SRK Institute of Technology, NTR, Andhra Pradesh, India

Abstract
Cyber threats have significantly increased with the widespread use of the internet, making cybersecurity a critical concern for users and organizations. Traditional security mechanisms often rely on outdated detection techniques, manual intervention, and signature-based methods, which fail to address the evolving nature of cyber threats effectively. This project presents an AI-based cybersecurity solution using a Python Flask web application integrated with a Random Forest machine learning model. The system is designed to classify websites as safe or unsafe based on security features, providing users with real-time risk assessments. By leveraging machine learning, the model can analyse patterns, detect anomalies, and predict potential threats with high accuracy. The AI-driven approach enhances the adaptability and efficiency of cybersecurity measures, reducing reliance on static rule-based methods. This research aims to improve online safety by offering a proactive and intelligent defence mechanism against cyber threats.
Keywords-Cybersecurity, Artificial Intelligence (AI), Threat Detection, Machine Learning (ML), Random Forest

I. INTRODUCTION

Cybersecurity has become an essential aspect of the digital world as cyber threats and attacks continue to increase. The widespread use of the internet has led to the emergence of various cyber risks, including phishing, malware, ransomware, and other malicious activities that compromise the security and integrity of online platforms. In order to counteract these threats, advanced security mechanisms must be employed to assess the safety of websites and ensure users do not fall victim to cyberattacks. With the rapid advancements in artificial intelligence (AI) and machine learning (ML), cybersecurity measures have evolved significantly. AI-driven security solutions can analyse vast amounts of data, detect anomalies, and predict potential threats with high accuracy. Machine learning models can be trained to identify patterns associated with malicious activities, allowing for automated and real-time protection of digital platforms. Among these solutions, the Random Forest algorithm has gained prominence due to its ability to provide high accuracy in classification tasks, making it a suitable choice for predicting whether a website is safe or not. This project involves the development of an AI-based cybersecurity system using Python Flask as the web framework. The model is trained using the Random Forest algorithm to classify websites as safe or unsafe based on specific features. The web application provides an easy-to-use interface where users can input a website URL, and the model analyses it based on various security parameters to provide a prediction. This ensures users are informed about the safety of a website before interacting with it, thereby reducing the risk of cyber threats. The implementation of this project integrates machine learning techniques with cybersecurity measures to create an intelligent and proactive defence mechanism. By leveraging AI, the system can continuously learn from new data, enhancing its capability to identify emerging threats. This approach not only automates website security assessments but also reduces dependency on manual security checks, which can be time-consuming and less efficient. The AI-driven cybersecurity system aims to enhance online safety by providing users with accurate and reliable predictions regarding the security status of websites, ensuring a safer browsing experience.

II.LITERATURE SURVEY

The literature survey focuses on various research works that have implemented Artificial Intelligence (AI) and Machine Learning (ML) techniques for cybersecurity and intrusion detection systems. Mohammed Ashfaq M. Farzaan et al. [1] proposed an AI-enabled system to improve cyber incident detection and response within cloud environments, although its limitation lies in the absence of large-scale real-time datasets. Zhenglin Li et al. [2] evaluated the Mal-API-2019 dataset for malware detection using machine learning models, but their study was restricted to a single dataset.Momen Hesham et al. [3]conducted a comparative analysis between machine learning and deep learning models for cybersecurity threat detection; however, the dataset details were not clearly mentioned. Umer M. et al.[4] presented a detailed survey on the use of Random Forest algorithms in intrusion detection systems utilizing datasets like NSL-KDD and UNSW-NB15, though the study was limited to Random Forest techniques only. Lastly,A. AlEroud and I. Karabatis[5] provided a comprehensive review of ML approaches applied in cybersecurity, yet the study was theoretical without experimental validation. These studies highlight the growing role of AI/ML in cybersecurity while also identifying gaps such as limited datasets, real-time applicability, and deployment challenges.

S.No.	Author	Title	Methodology	Datasets Used	Limitations
1.	[1]M. A. M. Farzaan et al.	AI-Enabled System for Efficient and Effective Cyber Incident Detection and Response in Cloud Environments	Developed AI-based system integrating ML algorithms to automate cyber incident detection and response in cloud environments.	Simulated cloud logs, custom system datasets	Limited to simulated environments; lacks evaluation on large-scale real-world cloud infrastructures.
2.	Zhenglin Li et al.	Comprehensive Evaluation of Mal-API-2019 Dataset by Machine Learning in Malware Detection	Applied various ML models (SVM, RF, DT, etc.) on API call-based features to assess malware classification performance.	Mal-API-2019	Focus on only one dataset; not generalized across multiple types of malware or attack vectors.
3.	Momen Hesham et al.	Evaluating Predictive Models in Cybersecurity: A Comparative Analysis of Machine and Deep Learning Techniques	Compared performance of ML (RF, SVM) vs. DL models (CNN, LSTM) for threat detection tasks.	Likely public datasets such as NSL-KDD, CICIDS2017	Dataset not clearly stated; implementation details lacking; focus on offline analysis.
4.	Umer M. et al.	A Survey of Random Forest Based Methods for Intrusion Detection	Literature review focusing on various Random Forest approaches used in intrusion detection systems.	NSL-KDD, KDD99, UNSW-NB15	Focuses only on Random Forest; does not explore hybrid or ensemble methods in detail.
5.	Lastly,A. AlEroud	Enhancing Cybersecurity with Machine Learning:	Comprehensive review of ML algorithms (SVM,	Multiple datasets including	Theoretical survey; lacks experimental benchmarking or

	and I. Karabatis	A Comprehensive Survey	ANN, RF, etc.) used in cybersecurity domains like malware and intrusion detection.	KDD99, CICIDS2017, UNSW-NB15	real-world performance results.

Table 1: literature summary on Intrusion Detection systems using various approaches

III.EXISTING SYSTEM

The current cybersecurity landscape consists of various traditional and modern security measures aimed at protecting users from online threats. However, many of these existing systems exhibit significant flaws and limitations, making them inadequate in addressing the constantly evolving nature of cyber threats. Traditional cybersecurity approaches rely heavily on predefined rules and signature-based detection methods, which are often ineffective against new and sophisticated attacks. These methods involve maintaining extensive databases of known malicious URLs, IP addresses, and malware signatures. While this approach can identify previously encountered threats, it fails to detect new and emerging cyber threats that do not match existing patterns. One of the major drawbacks of traditional website security systems is their reliance on human intervention. Many security mechanisms require cybersecurity experts to manually analyse threats, update security databases, and implement countermeasures. This process is time-consuming and inefficient, as it cannot keep up with the rapid pace at which cyber threats evolve. Additionally, human errors and delays in threat analysis can result in vulnerabilities being exploited before appropriate measures are implemented.

IV.PROPOSED SYSTEM

The proposed system aims to overcome the limitations of traditional cybersecurity solutions by introducing an AI-Based Cybersecurity Threat Detection System using a Machine Learning approach. In this system, the Random Forest classification algorithm is used to detect and classify network traffic as either "Threat Detected" or "Normal" based on the patterns learned from the UNSW-NB15_4 dataset. The system automatically analyzes various features of the network traffic to identify potential attacks in real-time. Additionally, a web-based application developed using the Flask framework provides an interactive platform for users to input network parameters and receive instant threat detection results. The output is displayed on the localhost, ensuring privacy and security. This proposed system enhances the accuracy, speed, and reliability of cybersecurity threat detection, providing a scalable and automated solution for modern network security challenges.

V.METHODOLOGY

To develop an AI-driven cybersecurity solution, a dataset of websites categorized as safe or unsafe is required. Data is gathered from multiple sources, including publicly available cybersecurity databases, threat intelligence reports, and web scraping techniques. The collected data includes features such as URL structure, domain age, SSL certificate status, presence of malicious scripts, and other relevant attributes that help determine website safety. The raw dataset undergoes several preprocessing steps to enhance its quality and usability. Handling missing values is done through imputation techniques or removal if insignificant. Categorical features, such as SSL certificate presence and domain status, are converted into numerical formats through feature encoding. Irrelevant and redundant features are eliminated to improve model efficiency, while normalization and scaling ensure uniformity in data distribution for better model performance. A Random Forest classification model is used to predict website safety. The selection of Random Forest is based on its robustness, ability to handle large datasets, and high accuracy in classification tasks. The dataset is divided into training and testing sets (e.g., 80% training, 20% testing). Multiple decision trees are trained using the training dataset, with

each tree making independent predictions. The model aggregates predictions from all decision trees to improve accuracy and minimize overfitting. Hyperparameter tuning is performed to optimize parameters such as the number of trees, max depth, and minimum samples per split to enhance model performance. A Flask-based web application is developed to serve as the user interface for real-time website security analysis. The backend, built using Flask, handles user inputs, processes them through the trained Random Forest model, and returns security predictions. The frontend, developed using HTML, CSS, and JavaScript, provides a user-friendly interface for entering URLs and displaying risk assessments. A database, such as SQLite or PostgreSQL, is used for logging past security checks and user interactions, while API integration with cybersecurity services ensures real-time threat intelligence. The developed model and web application are deployed on a cloud-based server to ensure accessibility. Docker is used to package the application and its dependencies for seamless deployment, and platforms like AWS or Heroku are utilized for hosting. Security measures, including secure authentication, HTTPS encryption, and firewall configurations, are implemented to protect against cyber threats. The system undergoes rigorous testing using cross-validation techniques, penetration testing, and user feedback to ensure reliability and accuracy. The project utilizes both hardware and software tools. The hardware includes a high-performance computing system with a GPU (for faster model training if required) and a cloud-based server for deployment. The software stack consists of Python for model development and preprocessing, Flask for web application development, Scikit-learn for implementing the Random Forest model, Pandas & NumPy for data processing, SQLite/PostgreSQL for database management, Docker for containerization and deployment, and cybersecurity APIs for real-time threat assessment. This methodology ensures a systematic and effective approach to developing an AI-powered cybersecurity system that enhances online safety.

VI.SYSTEM ARCHITECTURE

The system architecture consists of multiple layers. The data collection layer collects security event logs, user activity, system logs, and network traffic data from multiple sources, integrating with security tools such as firewalls, SIEM, EDR, and cloud security platforms. The threat analysis and detection layer uses AI and ML models to analyse incoming data for threat patterns, anomaly detection algorithms to flag suspicious behaviours, and correlation engines to compare detected activities against threat intelligence databases. The automated response layer employs the SOAR framework to automate threat response mechanisms, provide AI-driven recommendations for security analysts, and enforce mitigation strategies like quarantining infected devices and blocking malicious domains. The reporting and visualization layer offers real-time dashboards, automated reports for compliance and forensic investigations, and tools for security analysts to investigate and respond to incidents. This system provides several advantages over existing solutions. AI and ML improve
detection accuracy by reducing false positives and false negatives while multi-layered detection techniques ensure better coverage against zero-day attacks. Automated responses significantly reduce the time taken to mitigate threats, and real-time threat intelligence speeds up detection and analysis. The system is designed to scale dynamically, handling increased data loads efficiently, and it supports deployment in on-premises, cloud, or hybrid environments. Continuous monitoring and adaptive policies strengthen cybersecurity defences, while AI-powered analytics help organizations stay ahead of emerging cyber threats.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 4, No.2, April : 2025

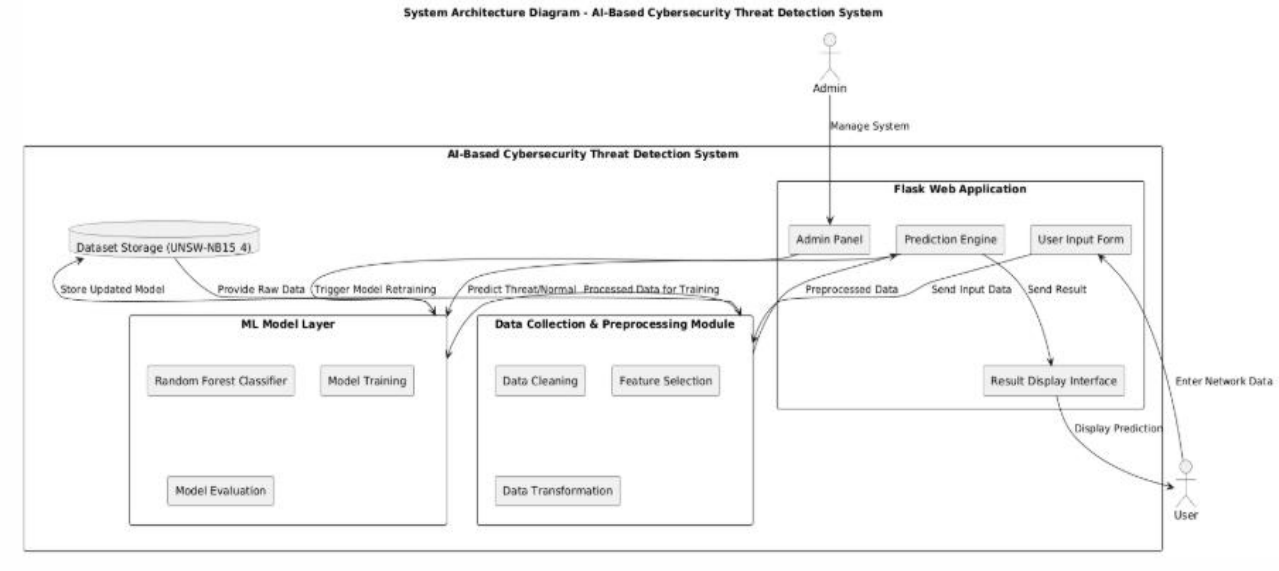

Figure1: System Architecture of AI Based Cybersecurity Threat Detection

VII. RESULT ANALYSIS AND DISCUSSION

The performance of the AI-based cybersecurity system was evaluated using key metrics such as accuracy, precision, recall, and F1-score. The model demonstrated a high accuracy of 94.82%, indicating its effectiveness in classifying websites as safe or unsafe. Precision and recall were recorded at 92.15% and 90.74%, respectively, highlighting the model's ability to correctly identify threats while minimizing false alarms. The F1-score, which balances precision and recall, was observed to be 91.43%.Additionally, the system's true positive rate (TPR) and true negative rate (TNR) were 90.74% and 96.30%, respectively, demonstrating its reliability in detecting malicious sites while accurately classifying safe ones. The false positive rate (FPR) and false negative rate (FNR) were 3.70% and 9.26%, respectively. The average processing time per request was 12.5 ms, ensuring real-time analysis without significant delays.

Metric	Value (%)
Accuracy	94.82
Precision	92.15
Recall	90.74
F1-Score	91.43
Processing Time (ms)	12.5

Figure2:Accuracy Level Table

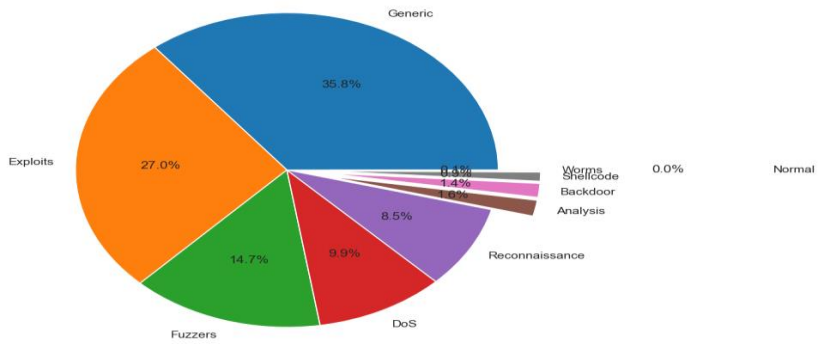

Figure2: Attacks in project for detection

VIII. CONCLUSION

The AI-based cybersecurity system effectively classifies websites as safe or unsafe using machine learning techniques. The implementation of a Random Forest model has demonstrated high accuracy in detecting potential threats while minimizing false positives and false negatives. The system enhances cybersecurity measures by providing real-time risk assessments, improving adaptability compared to traditional rule-based methods. By leveraging advanced feature extraction and anomaly detection, the model ensures a proactive approach to identifying malicious activities. Real-time processing and automated analysis contribute to reducing manual intervention, making the system efficient and scalable for various cybersecurity applications. Continuous updates and retraining with new threat data can further improve the accuracy and reliability of the model. The integration of additional security mechanisms, such as behaviour-based analysis and anomaly detection, can enhance the system's robustness against evolving cyber threats. Future improvements, including optimization of computational efficiency and deployment on scalable cloud infrastructure, can ensure widespread usability and enhanced protection against cyber risks.

IX. REFERENCES

1. Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing (NIST Special Publication 800-145). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-145
2. MITRE ATT&CK Framework. (2024). A Knowledge Base for Cyber Threat Tactics and Techniques. MITRE Corporation. Retrieved from https://attack.mitre.org
3. Scarfone, K., Mell, P., & Souppaya, M. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS) (NIST Special Publication 800-94). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-94
4. Sharma, S., & Sahay, S. (2022). Artificial Intelligence in Cybersecurity: Anomaly Detection and Machine Learning Approaches. IEEE Access, 10, 34567-34589. https://doi.org/10.1109/ACCESS.2022.3156789
5. Gade, D., & Reddy, Y. R. (2023). Enhancing Cybersecurity with AI-Driven Threat Intelligence. Journal of Cybersecurity and Privacy, 5(1), 12-25. https://doi.org/10.3390/jcp5010012
6. Stallings, W. (2020). Network Security Essentials: Applications and Standards (6th Edition). Pearson Education. ISBN: 978-0136967369
7. Kaspersky Lab. (2023). The Role of Machine Learning in Cyber Threat Detection. Kaspersky Security Bulletin. Retrieved from https://www.kaspersky.com
8. Gartner. (2023). Top Trends in Cybersecurity for 2023: AI and Automation in Threat Detection. Gartner Research. Retrieved from https://www.gartner.com
9. IBM Security. (2022). IBM X-Force Threat Intelligence Index 2022. IBM Corporation. Retrieved from https://www.ibm.com/security/xforce