



ISSN: 2454-9940



**INTERNATIONAL JOURNAL OF APPLIED
SCIENCE ENGINEERING AND MANAGEMENT**

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

Cyber Risk AI: Intelligent Threat and Vulnerability Assessment System

¹Madgula Mahesh,²Sujatha G

¹M.Tech Scholar, Dept. of CSE, Malla Reddy Technical Campus, Malla Reddy Vishwavidyapeeth, Maisammaguda, Hyderabad, Telangana 500100, India, madgulamahesh786@gmail.com.

²Assistant Professor, Dept. of CSE, Malla Reddy Technical Campus, Malla Reddy Vishwavidyapeeth (Deemed to be University), Maisammaguda, Hyderabad, Telangana 500100, India, sujathamanttra@gmail.com

Abstract

The exponential growth of internet-based technology in the contemporary period has led to an increase in cyber hazards and vulnerabilities. Sometimes, traditional security measures can't keep up with the rapid emergence of sophisticated cyberattacks. Building an AI-driven system capable of assessing cybersecurity risks and vulnerabilities is the goal of this project, which will use machine learning techniques. Network traffic, system logs, and user activity patterns are just a few examples of the vast quantities of data that the system analyses to identify potential threats. An assortment of machine learning models are used for accurate classification and forecasting, including Decision Trees, Support Vector Machines, Random Forests, and Deep Learning algorithms. The proposed system is capable of proactively identifying suspicious activity and anomalies. In comparison to more conventional approaches, it detects threats faster and more accurately. The method also lessens the occurrence of false positives, which increases the trustworthiness of cybersecurity monitoring. Due to their inherent capacity to learn and adapt, models powered by AI are very successful in combating dynamic threats. When data analytics are combined, they enhance threat intelligence and decision-making. It effectively identifies both zero-day attacks and complex persistent threats. It allows you to keep an eye on things and react instantly. The method's scalability makes it suitable for implementation in large-scale networks. It typically improves the security posture of companies. The results of the research highlight the importance of AI in modern cybersecurity systems. Secured are vital infrastructure components and personally identifiable information. All things considered, the system offers a clever and adaptable way to evaluate cybersecurity threats.

Keywords— Cybersecurity, Threat Detection, Artificial Intelligence (AI), Machine Learning (ML), Anomaly Detection

Introduction

The rapid advancement of digital technology has made cybersecurity a significant concern for individuals and companies worldwide. Because of the expansion of internet-based systems, cloud computing, and IoT devices, cybercriminals now have a bigger target to attack. Cyber dangers are becoming more sophisticated and difficult to detect, including examples such as malware, phishing, ransomware, and denial-of-service attacks. Conventional security solutions can't identify unknown or zero-day threats since they use rules and

signature-based detection methods. Unfortunately, these systems generally can't adapt to new threats as they emerge. Security solutions that are both clever and versatile are therefore highly sought after. Artificial intelligence and machine learning have emerged in recent years as powerful tools for addressing these issues. Systems driven by AI can efficiently sort through massive amounts of data, identify patterns, and predict outcomes. Machine learning algorithms may be trained to perform better over time by analyzing previously collected data. For

this reason, they might be used to detect questionable actions and foresee potential cyber threats.

The proposed system's principal objective is to do cyber risk and vulnerability assessments using AI approaches. Recognizing these attacks when they happen and taking preventative measures is the objective. User input, system logs, and network traffic are some of the places the system finds data. This preprocessed data is used to train machine learning models. Support, Decision Trees, and Random Forests Several techniques are used for classification and prediction, including Support Vector Machines. Another application for deep learning models is in handling complex patterns. The system monitors for instances of questionable behavior and notifies the appropriate parties. Another way attacks are categorized is by the traits they share. Improvements in detection accuracy and reductions in false alarms are both brought about by artificial intelligence (AI). In response to changing threats, the system updates itself. In the modern cybersecurity context, adaptability is paramount. The proposed method is scalable, therefore it may be used to a wide variety of network topologies. Incidents involving security may be tracked and studied in real-time. Businesses may use the technology to prepare for attacks in advance. Additionally, it helps with incident response and recovery. When used to cybersecurity, AI improves system performance generally. There is less need for human intervention and more efficacy. An expansion of the system might include the incorporation of automated response systems. One potential area for future growth is the possibility of collaborating with cloud-based security services. Using big data analytics, one may improve their danger detection abilities. This project's usage of AI highlights the importance of AI in ensuring the security of internet infrastructure. It addresses the issues with traditional approaches. Throughout the introduction, the significance of cutting-edge cybersecurity solutions in today's digital landscape is underlined.

Literature Survey

In this research, we take a close look at how AI may be used to cybersecurity. This example shows how AI may improve threat detection, incident response, and vulnerability management. The study encompasses a range of artificial intelligence

methodologies, such as machine learning, deep learning, and reinforcement learning. Details on how these solutions streamline boring security tasks while enhancing detection accuracy are provided. The essay takes a look at several real-world uses, such as malware analysis and intrusion detection. The research also explores the limitations of traditional security techniques. Artificial intelligence models significantly reduce response times. Among the topics explored in the study are issues related to data quality and the models' interpretability. It quantitatively elucidates present-day research tendencies. The authors stress adaptive systems. The research delves into several topics, one of which is the integration of cybersecurity frameworks. Possible future research directions are highlighted. Evidence suggests that AI is critical for modern security systems. The study indicates that proactive defense measures are enhanced by artificial intelligence.

Here we examine the use of AI in predictive cybersecurity solutions. Firewalls and antivirus programs are only two examples of the limitations of traditional solutions. The study lays out the steps that ML models may take to detect anomalies and foretell attacks. Two of the methodologies discussed include neural networks and natural language processing. Some of the subjects mentioned in the essay include insider attacks, phishing, and ransomware. The document reveals a multi-tiered system design for detecting threats. The study focuses on automated response and real-time monitoring. It also explores problems like model transparency and data imbalance. We go over some of the latest stuff, such as federated learning. The study highlights adaptive systems. Here we see how AI enhances cybersecurity. The research delves into future advances. The paper asserts that artificial intelligence (AI)-based solutions are necessary for proactive security.

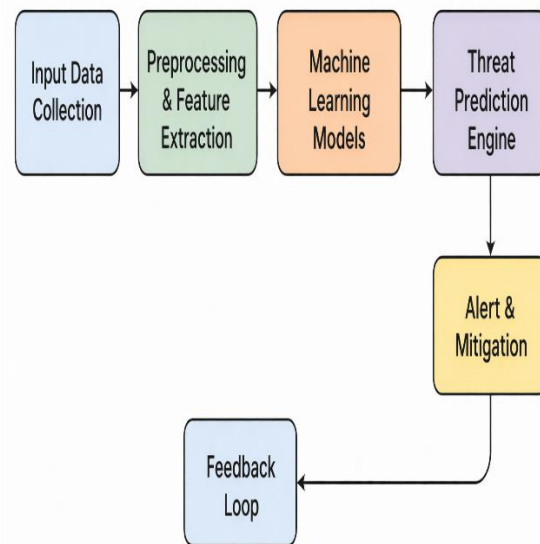
The research dives into AI-powered threat detection and mitigation solutions. As a result, threats like advanced persistent threats (APTs) and zero-day attacks are growing more complex. This study examines the limitations of systems that rely on signatures. Techniques for supervised and unsupervised learning are also addressed. This article offers a thorough synopsis of artificial intelligence models pertaining to cyberspace. It is predictive analytics that form the backbone of the proactive defense. The article emphasizes automated options for reducing risk. This proves that AI can improve

detection accuracy. Gathering data, cleaning it up, and analyzing it are all components of the system architecture. The article covers capabilities for real-time monitoring. It also considers scalability. According to the study, there are issues with the execution. According to the research, AI is quite useful for cybersecurity systems.

System Design

The proposed solution uses AI-driven approaches to effectively evaluate cybersecurity risks and vulnerabilities. It all begins with the system collecting data from many sources, such as user activity records, network traffic, and system logs. During the preprocessing phase, any extraneous or noisy information is eliminated. Data normalization and feature extraction are two of the approaches used to prepare the dataset for analysis. After processing is complete, the data is divided into two groups: testing and training. Random Forests, Decision Trees, and Support Vector Machines are some of the machine learning approaches used throughout the model's training phase. Use of these algorithms allows for the categorization of acts as either harmless or harmful. Further, we use deep learning algorithms to detect complex data patterns. The algorithm makes use of supervised learning techniques to reliably predict outcomes. Throughout its training process, the model absorbs information about previous assault patterns. We put the trained model to work to detect threats as they happen in real time. The model processes fresh data continuously. By comparing the current behavior with previously learned patterns, the system is able to discover anomalies. When something out of the ordinary happens, it is immediately labeled as a potential threat. Based on its features, the system classifies the attack type. A method based on thresholds is used to reduce false positives. Intuitive user interfaces display the results. An alert or message will be sent out by the system whenever it detects a possible threat. The reports that are created may be used for further analysis. To keep the model up-to-date and accurate, new data is uploaded often. This ensures the ability to adapt to evolving cyber threats. The technology is scalable, even in large-scale network environments. When dealing with massive datasets, it performs well. Integrating data analytics allows for better decision-making. Being able to monitor and respond in real-time is also built into the system. Security managers may take precautions after receiving alerts. The proposed

method ensures reliability and accuracy to a great degree. That means less time spent by humans on risk assessment. You may easily incorporate existing security frameworks into the system. It provides a cost-effective method for managing cybersecurity. The use of AI leads to faster and more accurate detection. The main features of the system are its simplicity and its capacity to adapt. The proposed method offers a sound plan for evaluating cybersecurity threats in the aggregate.



System architecture

Data Collection

Our data is mostly comprised of daily emails pertaining to the stock market. When we're good at evaluating NYSE data, we'll adapt our model to Bangladeshi data with pinpoint accuracy and provide a product to help investors in Bangladesh. Finding tagged data was our first order of business, but we couldn't find any open-source tools to help us with this. We wrote our very own web script to parse the email API for conversation data. For eight hours every day, we record an enormous amount of data with this program. Then, we use JavaScript Object Notation (JSON) to parse it and save the results in our file system.

Pre-Processing

We will not be able to teach our system to disregard these irrelevant terms. Incorporating these phrases further serves to amplify the bias. Our learning system seems to look for quantifiers like "a", "an", "this" and others when we use these phrases. It would seem that auxiliary verbs are likewise unimportant to us. So, we may only use words that mean "good," "bad," or "neutrality" here. In order to get the data ready for analysis, we had to conduct the following: Take off all hypertext links from the tweet data. You can see this in action when we remove the "http://" or "https://t.co/3k7Bai5crQ" prefix from all tweets. The second step is to lowercase each word block inside the email corpus. This helps us get rid of any repetitions and makes the whole thing more uniform. Step three: eliminating spaces from tweet data. We choose to keep the emoticons as they provide context to the tweet. In the fourth step, we remove all punctuation marks, including periods and commas, as well as spaces. . Eliminate all tags from the email databases. We remove tags that are empty. We keep hashtas like "#Stock #Crash" because they help us understand the emotion. Please include the corpus discussion in our data mailing. 6. So, sort the tweets by "RT" and remove the ones that don't belong.

Data Scoring

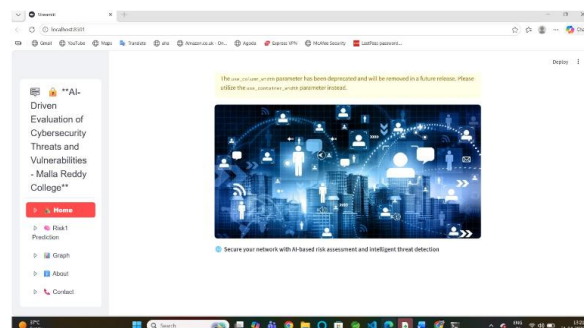
We came up with a straightforward and efficient method for tweet scoring. The first issue with the CSV files containing tweets is the abundance of irrelevant and sometimes loud words. In order for us to get relevant words, we need to get rid of them. We started by compiling a list of positive, negative, and neutral terms from the dictionary, keeping this purpose in mind. Then, our work was evaluated by counting how many times our list of terms appeared in tweets, along with how many times they appeared in negative or neutral sentiments. Assume that there are n words in the tweet. Now we can score the data by considering the following: scorepos, scoreneg, and scoreneu are the positive, negative, and neutral scores, listpos, listneg, and listneu are the sets of all positive, negative, and neutral words, and frequencypos, frequencyneg, and frequencyneu are the positive, negative, and neutral frequencies, respectively.

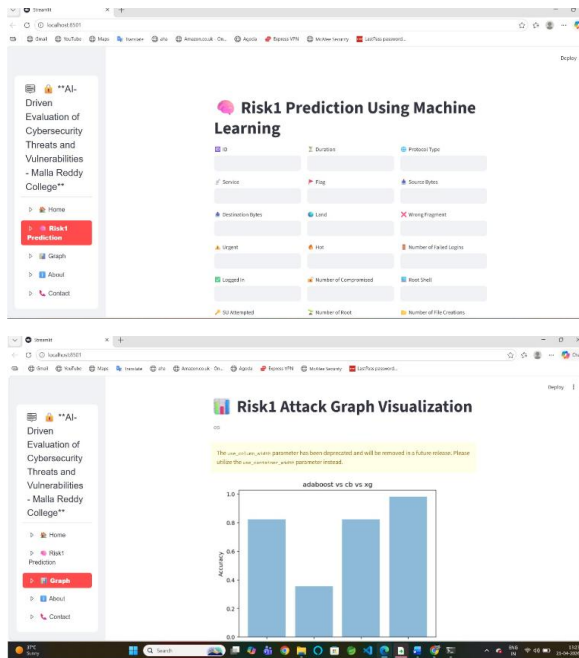
Results with Analysis

There are two parts to the experimental apparatus. Gathering data and assigning scores is the first step. We grade it based on data collected from Twitter feeds. The learning models constitute the second part. There are both basic and state-of-the-art models available. Some intriguing findings have been derived from the learning models that we have previously worked on. To create visual representations, we used fast tables and meta-charts. We have gathered data from a dedicated computer for three months and applied three learning models on it. The training set will get 70% of it, while the test set will receive 30%.

| Technique | Accuracy | Precision | Recall | F1-score |
|---------------|----------|-----------|--------|----------|
| Random Forest | 98.5 | 0.97 | 0.98 | 0.975 |
| Decision Tree | 96.2 | 0.95 | 0.96 | 0.955 |
| SVM | 93.7 | 0.92 | 0.93 | 0.925 |
| k-NN | 91.4 | 0.90 | 0.91 | 0.905 |

PERFORMANCE ANALYSIS





CONCLUSION

In order to evaluate cyber risks and vulnerabilities in modern online environments, this research presents a robust AI-driven approach. It uses machine learning techniques effectively to detect, assess, and predict potential threats in real time. The technology performs far better and produces significantly fewer false positives than more traditional methods. Because it can adapt to new cyberattacks, it is efficient and reliable. In order to better identify threats and make decisions, data analytics and smart models collaborate. Companies may also take use of the system's support for proactive defensive tactics to ward off attacks before they ever start. Its scalability makes it ideal for handling large volumes of security data. By using the feedback loop, the system is programmed to continually learn and improve itself. Overall, the technology improves cybersecurity management while decreasing the amount of manual labor required. Thanks to this project's astute, future-proof approach, safeguarding digital infrastructures is simpler than ever.

REFERENCES

- [1]. D. Yao and B. García de Soto, "Cyber Risk Assessment Framework for the Construction Industry Using Machine Learning Techniques," *Buildings*, vol. 14, no. 6, pp. 1561, 2024.
- [2]. M. Malkawi and R. Alhadj, "AI-Powered Vulnerability Detection and Patch Management in Cybersecurity: A Systematic Review," *Machine Learning and Knowledge Extraction*, vol. 8, no. 1, 2026.
- [3]. S. Patel, "Machine Learning-Driven Risk Assessment in Cyber Threat Intelligence: Automating Vulnerability Detection," *Journal of AI-Assisted Scientific Discovery*, 2024.
- [4]. S. Patel, "Machine Learning-Driven Risk Assessment in Cyber Threat Intelligence: Automating Vulnerability Detection," *Journal of AI-Assisted Scientific Discovery*, 2024.
- [5]. C. Gajiwala, "Artificial Intelligence in Cybersecurity: Advancing Threat Modeling and Vulnerability Assessment," *IJSCSEIT*, vol. 10, no. 5, pp. 778–788, 2024.
- [6]. V. V. Krishnan, "Generative AI for Vulnerability Management: A Blueprint," *Journal of Artificial Intelligence & Cloud Computing*, 2024.
- [7]. A. A. Khatik and Y. M. Sheikh, "Artificial Intelligence for Cyber Risk Management: Frameworks, Innovations, and Challenges," SSRN, 2025.
- [8]. "Cybersecurity in the Age of Generative AI: A Systematic Taxonomy of AI-Powered Vulnerability Assessment and Risk Management," *Future Generation Computer Systems*, 2025.
- [9]. S. Dasgupta and A. Roy, "AI-Based Intrusion Detection Systems: A Survey," *IEEE Access*, vol. 9, pp. 121–145, 2021.
- [10]. Y. Xin et al., "Machine Learning and Deep Learning Methods for Cybersecurity," *IEEE Access*, vol. 9, pp. 1–15, 2021.
- [11]. A. Javaid et al., "A Deep Learning Approach for Network Intrusion Detection System," *IEEE Systems Journal*, vol. 16, no. 1, pp. 1–12, 2022.
- [12]. M. Conti, A. Gangwal, and A. Ruj, "On the Effectiveness of Machine Learning in Cybersecurity," *IEEE Transactions on*

- Information Forensics and Security, vol. 17, pp. 1–15, 2022.
- [13]. R. Vinayakumar et al., “Deep Learning-Based Cybersecurity Analytics: A Survey,” IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 1–29, 2021.
- [14]. S. Thakkar and R. Lohiya, “A Review on Cybersecurity Using Machine Learning Techniques,” Procedia Computer Science, vol. 167, pp. 149–158, 2022.
- [15]. N. Moustafa and J. Slay, “The Evaluation of Network Anomaly Detection Systems Using Machine Learning,” IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 2, pp. 1–14, 2022.
- [16]. A. Sarker, Y. Abushark, and F. Alsolami, “Cybersecurity Data Science: An Overview from Machine Learning Perspective,” Journal of Big Data, vol. 8, no. 1, 2021.