Automated Cyber Threat Identification Using Natural Language Processing

Parumanchala Bhaskar, Kandukuri Ramachari, Shaik Arbas Basha, Kamireddy Vivekananda Reddy, Bandi Malleswara Reddy and Suravi Ravi Teja
Department of Computer Science and Engineering, Santhiram Engineering College, Nandyal, Andhra Pradesh, India

Keywords: Intelligence on Cyber Threats, Cybersecurity, Natural Language Processing (NLP), Automated Threat Recognition, Analysis of Threats, Machine Learning, Deep Learning, Information Mining, Extraction of Information.

Abstract: This abstract paper addresses this challenge through the application of Natural Language Processing (NLP) to facilitate the automation of cyber threat detection. The suggested system uses modern NLP methods to interpret large volumes of textual data from sources including cybersecurity reports, social media, forums and dark web conversations. In an increasingly digital world, cyberthreats are becoming more common and present a major security and privacy threat. As malevolent behaviour is dynamic, most conventional threat detection mechanisms tend to lag. The solution aims to enhance the resilience of digital infrastructures against cyberattacks by improving the precision, effectiveness, and scalability of threat detection. As there are rapid dynamics of the digital world, the cyberattacks are also growing to be more sophisticated and bigger than ever. This research will solve this basic problem by creating a mechanised system for cyber threat identification using some Natural Language Processing (NLP). The solution aims to strengthen the defences of digital infrastructures against cyberattacks by increasing the precision, effectiveness and scalability of threat detection.

1 INTRODUCTION

The Problem: We have tons of information about potential cyber threats. This information is scattered everywhere – in security logs, reports, social media, etc. It's too much for humans to handle, and it's hard to find the real threats quickly. Plus, the threats are always changing.

The Solution: NLP can help! Think of NLP as teaching computers to understand human language. Rather than simply focusing on words, computers have the ability to grasp the meaning behind the words.

How NLP Assists: Makes Sense of the Data: NLP can analyse all that intricate threat data (logs, reports, posts) and decipher it. It's akin to having a super-fast reader who understands what it is reading. NLP is a branch of artificial intelligence that focuses on analysing, comprehending, and producing the languages that people naturally use to facilitate computer interactions using human natural languages instead of computer languages. Natural language processing allows computers to interact in a manner akin to human speech.

Discovers Patterns: NLP is capable of uncovering hidden patterns and clues that might suggest a cyber-attack is happening or is about to happen. It has the ability to recognize connections that humans might overlook. NLP allows computers to comprehend and process large amounts of text data to identify cyber threats more efficiently and swiftly than humans can do alone. It's like giving cybersecurity experts a powerful assistant that can read and understand everything!

2 LITERATURE REVIEW

Web applications in the current era play an extremely crucial part in personal life as well as in the progress of any nation. Web applications have experienced an extremely fast evolution during the recent years and their acceptance is increasing at a quicker pace than was anticipated some years ago. In these days,

Bhaskar, P., Ramachari, K., Basha, S. A., Reddy, K. V., Reddy, B. M. and Teja, S. R.
Automated Cyber Threat Identification Using Natural Language Processing.
DOI: 10.5220/0013887300004919

In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 2*, pages 614-619
ISBN: 978-989-758-777-1

trillions of transactions are made online with the help of various Web applications. Although these applications are accessed by hundreds of users, in most instances the security level is low, and hence they are prone to get compromised. In the majority of the scenarios, a user must be authenticated before any communication is made with the backend database. An arbitrary user must not be granted access to the system without evidence of valid credentials. Nevertheless, a crafted injection provides access to unauthorized users. This is primarily achieved through SQL Injection input. Despite the emergence of various methods to avoid SQL injection, it continues to be a threatening issue for Web applications. In this paper, we have provided an in-depth survey on various SQL Injection vulnerabilities, attacks, and prevention methods. Besides discussing our results from the research, we also write down future prospects and potential evolution of countermeasures for SQL Injection attacks.

The Internet is Important but RiskWe rely on the internet for everything, but it's also full of dangers like cyberattacks.

Threat Intelligence Helps: To fight these attacks, we use "threat intelligence". This is like gathering clues about upcoming attacks, including details regarding the attacker's methods ("signatures"). This prepares us. Where We Obtain Clues: We gather these clues from different places:

Formal Sources: Authorized organizations that share threat information in a methodical, organized way (like a formal report).

Informal Sources: More casual sources, such as news articles, blogs, or discussions.

Organized Clues are Ideal: When the clues are structured ("organized"), security tools can more readily understand them and take automated measures to keep us protected.

In summary: We collect signs of cyberattacks from multiple sources. The more organized these pieces of information are, the more effectively we can shield ourselves. However, the slide indicates that there remains a significant amount of unstructured, chaotic information that is challenging to utilize, and that's where the new danger arises.

3 EXISTING RESEARCH

Current research has examined multiple aspects of NLP-based cyber threat detection, including: Automated phishing identification using machine learning techniques.

Real-time threat surveillance on social media utilizing NLP strategies.

Automated extraction of threat intelligence from security documents. Implementation of message queuing and stream processing for handling large data volumes. Studies have also explored the use of NLP models in cloud environments to achieve scalability and efficiency.

Drawback in Existing System:

Contextual Noise: A lot of natural language depends on context and has ambiguity. Potentially, the same name or term can have different meanings based on context, creating difficulties in prediction and makeup of evolving cyber threats.

Domain-Specific Models: Most of NLP models do not generalize well across domains.

sectors, or languages. A model which might have trained up to a specific data category may differ completely in another scenario.

Extractable knowledge and Trust: Natural Language Processing models are often described as black-boxes, and these are not straightforward for us humans to interpret This ambiguity can erode trust and limit broad use.

Adversarial Attacks: Similar underlying to images, NLP models can fall victim to adversarial layouts where malicious actors intentionally shape input data to fool the model.

4 PROPOSED SYSTEM

The framework coordinates three fundamental elements: first, the identification of cyber threats and their classification; second, the profiling of these identified threats, distinguishing their motives and goals through a sophisticated machine learning architecture; and third, the issuance of alerts based on the danger posed by the identified threats. A significant innovation in our work lies in our approach to define these emerging threats, providing contextual understanding of their motives. This improved layer of understanding not only enhances threat detection but also offers avenues for effective countermeasures. In our experimental research, the profiling stage achieved an impressive F1 score of 77%, demonstrating a strong ability to identify and understand identified threats. " "This Paper leads the forefront of proactive cybersecurity strategies, aiming to equip defenders with a sophisticated system capable of performing early threat detection and advanced threat characterization. By utilizing a rich source of event data and advanced machine learning techniques, the framework not only identifies threats

but also delves deeper into their motives, providing valuable insights for proactive defence strategies against rapidly evolving cyber threats.

The Problem: The rising quantity and complexity of cyber threats necessitate automated and scalable solutions for early detection and mitigation. Traditional security systems that rely on manual analysis are ineffective and susceptible to human errors. Natural Language Processing (NLP) offers a powerful method to automate the identification of cyber threats from text data, enabling real-time analysis and proactive defence.

The Solution: Researchers created a system to combat them. It operates in three stages: Identify Threats: Recognizes and tags the threats to cyberspace.

Profile Threats: Establishes the intentions of the attacker using machine learning (a form of AI). This uncovers what the attackers intend to achieve.

Generate Alerts: Based on the threat's severity, alerts are generated by the system.

Main Idea: The core of this system is how it discerns what the attackers are trying to accomplish. Understanding the attackers' goals allows defenders to be better prepared and react effectively.

Advantages of Proposed System:

Real-time Threat Detection: NLP can process and analyse large volumes of unstructured data quickly. The sooner the threat is identified, the more opportunities organizations have to act to counter it before it can do damage.

Adaptability to Emerging Threats: NLP models can be continuously trained and updated to stay in line with evolving cyber threats. The system can remain relevant, compare and contrast its past decisions with new data & retraining the models at regular intervals to detect new threats.

Enhanced Situational Awareness: NLP systems increase situational awareness by processing and interpreting natural language. Organizations gain insight into the evolving threat landscape, adversarial techniques, and can take proper actions with regard to cybersecurity.

Cost-Effectiveness: Reduces manual labour by using NLP-automated threat detection that works on large volumes of text data. This economical approach enables organizations to optimize resource allocation and devote efforts to strategic cybersecurity initiatives.

5 METHODOLOGY

Data Collection and Preprocessing

A pipeline will be built to harvest text data around the web/post-processed. Text cleaning, tokenization, normalization, etc., will be automated in data preprocessing. TF-IDF, word embeddings are some of the techniques that will be used for feature extraction. Manh power from message queueing technologies will be used to process data streams.

Development and Deployment of NLP Models: "NLP models (for Machine Learning models and Deep Learning models) will be created for the identification and classification of threats. The models will be tuned to latency and throughput for real-time processing. Your models will be deployed at scale, such as in a cloud environment or containerized environment. "

Real-Time Threat Detection: A real-time threat detection system will be implemented, utilizing stream processing technologies. " The system will continuously analyse incoming data streams and trigger alerts for detected threats.

Evaluation Metrics: Accuracy, precision, recall, F1-score, latency, throughput, and scalability metrics.

6 ARCHITECTURES

Figure 1 illustrates the proposed architecture for cyber threat detection utilizing Natural Language Processing (NLP) techniques.

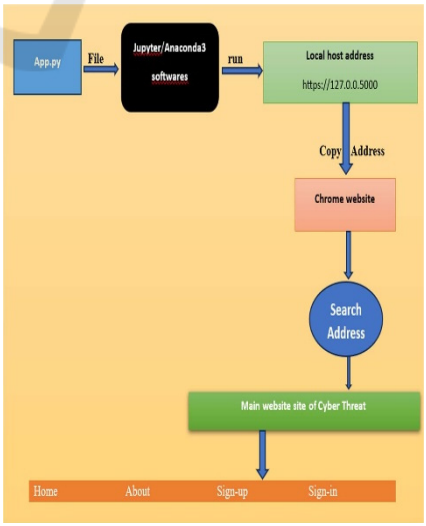

Figure 1: Architecture of cyber threat detection using NLP.

- Application File (App.py):

The process begins with an application file, denoted as App.py. This represents the user- initiated program or script designed to interact with the cyber threat platform.

- File Execution via Jupiter/Anaconda3:

The App.py file is executed using Jupiter Notebook or Anaconda3, which are powerful environments for Python development and data science.

- Local Host Address Generation:

Upon execution, the application generates a local host address, specifically https://127.0.0.5000.

- Address Copying:

The generated local host address (https://127.0.0.5000) is copied for subsequent access.

- Chrome Website Access

The copied address is subsequently used to launch the service via the Chrome web browser.

This clarifies the use of a standard web browser for engaging with the local service. The choice of Chrome indicates suitability and ease for the user

- Search Address Input:

The copied address is pasted into the browser's search bar or address field.

- Main Website of Cyber Threat Platform:

The browser navigates to the main website of the cyber threat platform, based on the provided address.

- Platform Interaction:

The platform offers various interactive options, including "Home," "About," "Sign-up," and "Sign-in."

7 EXPECTED OUTCOMES

This Paper aims to:

- Develop an automated framework for real-time cyber threat identification.
- Enhance the efficiency and effectiveness of threat detection through automation.
- Provide a scalable and adaptable solution for large-scale data analysis.
- Improve the speed of response to cyber threats.
- Future research will focus on:
- Integrating automated threat response capabilities.
- Improving the explainability of real-time threat detection models.
- Implementing adaptive learning techniques for continuous model improvement.
- Building a report to future screening of identified threats.

8 CONCLUSIONS

We researched a range of machine learning algorithms Naive Bayes, SVM, KNN, Random Forest, Bagging, Boosting, Neural Networks, and Voting Classifier in this research that are specifically well-suited for various classification and prediction tasks. These algorithms find

important applications across a range of fields from text classification and image recognition to anomaly detection and ensemble learning. What makes them work is their capability to manage complex data relationships, respond to differing datasets, and make accurate predictions. In the future, machine learning algorithms for applications such as cybersecurity, health diagnostics, and autonomous systems have promising prospects. Developments in deep learning and reinforcement learning are poised to make algorithms even better, allowing more advanced applications in real-world situations. Additionally, combining these algorithms with new technologies like edge computing and quantum computing could provide new paths for processing speed and accuracy.

9 FUTURE SCOPE

Future work may include optimizing such algorithms to run in real-time, enhancing explainability via model explainability methods and exploring how these can be combined with other new technologies such as blockchain for enhanced security and transparency in data-driven systems. More research work will also be directed towards improving the scalability of algorithms, adversarial robustness and addressing the ethical considerations in the deployment of AI systems in various domains.

10 RESULTS

The Figure 2 below represents the classification of Cyber Threat Types using the proposed model

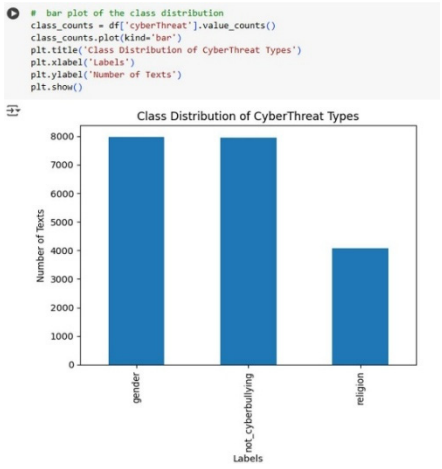

Figure 2: Class distribution of cyber threat types.

The below Figures 3 and 4 represents mostly used words and most frequently used words in the given dataset.

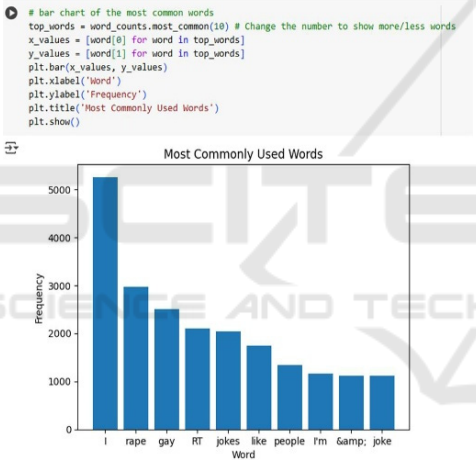

Figure 3: Most commonly used words.

Figure 4: Most frequent words used in texts.

The below Figures 5,6 and 7 shows the Process of NLP is Started, Cyber Threat Not Detected and Cyber Threat Detected.

```
#Natural Language Processing
#DATA CLEANING
# Clean the data
def clean_text(text):
    # Remove HTML tags
    text = re.sub('<.*?>', '', text)

    # Remove non-alphabetic characters and convert to lowercase
    text = re.sub('[^a-zA-Z]', ' ', text).lower()

    # Remove URLs, mentions, and hashtags from the text
    text = re.sub(r'http\S+', '', text)
    text = re.sub(r'@\S+', '', text)
    text = re.sub(r'#\S+', '', text)

    # Tokenize the text
    words = nltk.word_tokenize(text)

    # Remove stopwords
    words = [w for w in words if w not in stopwords.words('english')]

    # Stem the words
    stemmer = PorterStemmer()
    words = [stemmer.stem(w) for w in words]

    # Join the words back into a string
    text = ' '.join(words)
    return text
```

Figure 5: Process of NLP is started.

Figure 6: Cyber threat not detected.

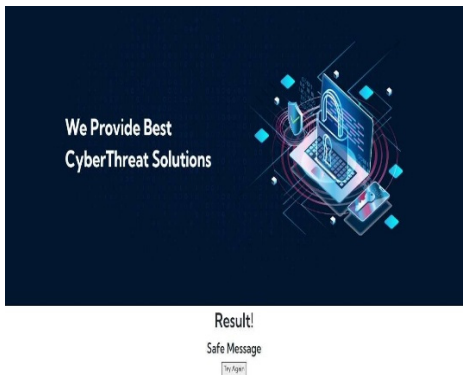

Figure 7: Cyber threat detected.

REFERENCES

Chaitanya, V. Lakshmi, and G. Vijaya Bhaskar. "Apriori vs Genetic algorithms for Identifying Frequent Item Sets." International journal of Innovative Research & Development 3.6 (2014): 249-254.

Chaitanya, V. Lakshmi. "Machine Learning Based Predictive Model for Data Fusion Based Intruder Alert System." journal of algebraic statistics 13.2 (2022): 2477-2483

Chaitanya, V. Lakshmi, et al. "Identification of traffic sign boards and voice assistance system for driving." AIP Conference Proceedings. Vol. 3028. No. 1. AIP Publishing, 2024

Devi, M. Sharmila, et al. "Machine Learning Based Classification and Clustering Analysis of Efficiency of Exercise Against Covid-19 Infection." Journal of Algebraic Statistics 13.3 (2022): 112-117.

Devi, M. Sharmila, et al. "Extracting and Analyzing Features in Natural Language Processing for Deep Learning with English Language." Journal of Research Publication and Reviews 4.4 (2023): 497-502.

Mahammad, Farooq Sunar, Karthik Balasubramanian, and T. Sudhakar Babu. "Comprehensive research on video imaging techniques." All Open Access, Bronze (2019).

Mahammad, Farooq Sunar, and V. Madhu Viswanatham. "Performance analysis of data compression algorithms for heterogeneous architecture through parallel approach." The Journal of Supercomputing 76.4 (2020): 2275-2288.

Mahammad, Farooq Sunar, et al. "Key distribution scheme for preventing key reinstallation attack in wireless networks." AIP Conference Proceedings. Vol. 3028. No. 1. AIP Publishing, 2024.

Mandalapu, Sharmila Devi, et al. "Rainfall prediction using machine learning." AIP Conference Proceedings. Vol. 3028. No. 1. AIP Publishing, 2024.

Mr. M. Amareswara Kumar, "Baby care warning system based on IoT and GSM to prevent leaving a child in a parked car" in International Conference on Emerging Trends in Electronics and Communication Engineering - 2023, API Proceedings July-2024.

Mr. M. Amareswara Kumar, EFFECTIVE FEATURE ENGINEERING TECHNIQUE FOR HEART DISEASE PREDICTION WITH MACHINE LEARNING" in International Journal of Engineering & Science Research, Volume 14, Issue 2, April-2024 with ISSN 2277-2685.

Paradesi Subba Rao, "Detecting malicious Twitter bots using machine learning" AIP Conf. Proc. 3028, 020073 (2024), https://doi.org/10.1063/5.0212693

Paradesi Subba Rao,"Morphed Image Detection using Structural Similarity Index Measure"M6 Volume 48 Issue 4 (December 2024),https://powertechjournal.com

Parumanchala Bhaskar, et al. "Machine Learning Based Predictive Model for Closed Loop Air Filtering System." Journal of Algebraic Statistics 13.3 (2022): 416-423.

Parumanchala Bhaskar, et al. "Incorporating Deep Learning Techniques to Estimate the Damage of Cars During the Accidents" AIP Conference Proceedings. Vol. 3028. No. 1. AIP Publishing, 2024.

Parumanchala Bhaskar, et al "Cloud Computing Network in Remote Sensing-Based Climate Detection Using Machine Learning Algorithms" remote sensing in earth systems sciences(springer).

Suman, Jami Venkata, et al. "Leveraging natural language processing in conversational AI agents to improve healthcare security." Conversational Artificial Intelligence (2024): 699-711.

Sunar, Mahammad Farooq, and V. Madhu Viswanatham. "A fast approach to encrypt and decrypt of video streams for secure channel transmission." World Review of Science, Technology and Sustainable Development 14.1 (2018): 11-28.