IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 2, February 2026

DOI: 10.17148/IJARCCE.2026.15248

ThreatSpeak: NLP-Driven Dark Web Intelligence Monitor

Dhaksha S[1], Dr. A. Nirmala[2]

Student, Department of Computer Science with Cognitive Systems, Dr. N.G.P Arts and Science College, Coimbatore, India[1]

Head, Department of Computer Science with Cognitive Systems, Dr. N.G.P Arts and Science College, Coimbatore, India[2]

Abstract: The rapid growth of cybercrime and dark web activities has made threat monitoring an essential task for cybersecurity analysts. Many organizations struggle to identify potential cyber threats quickly due to the large volume of unstructured textual data generated across various online sources. This project introduces **ThreatSpeak**, a machine learning-based system designed to analyze and classify cyber threat information from textual data. The system allows users to upload threat-related text files, which are automatically preprocessed and analyzed using natural language processing techniques. A trained machine learning model categorizes the content into relevant cyber threat types such as phishing, malware, or data breaches. In addition to classification, the system extracts threat indicators, identifies potential targeted assets, and generates a concise analytical summary to assist cybersecurity professionals in understanding the threat context. The application is implemented using **Python, Streamlit, and Scikit-learn**, providing a simple web interface for threat analysis. ThreatSpeak demonstrates how machine learning can support cybersecurity intelligence by improving the speed and accuracy of threat identification from textual sources.

Keywords: Cybersecurity, Threat Intelligence, Machine Learning, Natural Language Processing, Dark Web Monitoring

I. INTRODUCTION

The rapid growth of the internet and digital services has increased the number of cyber attacks targeting organizations, financial institutions, and individuals. Cyber criminals frequently use hidden networks and underground forums on the dark web to distribute malicious software, stolen credentials, and attack strategies. Traditional monitoring systems rely heavily on manual analysis, which is time consuming and inefficient when large volumes of threat information are generated daily. The ThreatSpeak system is designed to address this challenge by automating the analysis of threat related text data. The system uses Natural Language Processing techniques to preprocess and clean the text before applying a machine learning classification model. By automatically identifying the category of threat and extracting relevant intelligence indicators, the system helps security professionals gain insights into the nature of cyber attacks.

II. RELATED WORK

Several cybersecurity research efforts have explored the use of machine learning for threat detection. Previous studies have applied text mining and classification techniques to identify malicious activities from security reports and online discussions. Natural Language Processing models have been widely used to process unstructured threat intelligence data. Existing solutions often focus on network traffic analysis or malware detection. However, fewer systems are designed specifically for analyzing textual threat intelligence gathered from reports and dark web sources. ThreatSpeak contributes to this area by combining text preprocessing, machine learning classification, and intelligence extraction within a single automated system.

III. PROPOSED SYSTEM

The proposed ThreatSpeak system provides an automated platform for analyzing cyber threat information. The user uploads a text file containing threat related content. The system processes the input through multiple stages including text preprocessing, machine learning classification, intelligence extraction, and summary generation.

In the preprocessing stage, unnecessary characters and formatting elements are removed to normalize the text. The cleaned text is then converted into numerical feature vectors using the TF-IDF technique. A trained machine learning

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 2, February 2026
DOI: 10.17148/IJARCCE.2026.15248

model analyzes these vectors and predicts the most relevant threat category. The system also searches for predefined keywords related to common cyber threats and identifies targeted assets mentioned in the text.

IV. SYSTEM IMPLEMENTATION

The ThreatSpeak system is implemented using Python programming language. The Natural Language Processing tasks are handled through text preprocessing techniques such as lowercasing, punctuation removal, and tokenization. TF-IDF vectorization is used to convert textual information into numerical data suitable for machine learning models.

A classification model is trained using a labeled dataset containing various cyber threat categories. The trained model and vectorizer are stored and later used within the web application for prediction. The user interface is built using the Streamlit framework, which allows users to upload files and view analysis results directly through a web browser.

V. METHODOLOGY

The ThreatSpeak system follows a structured methodology to analyze textual cyber threat data and generate meaningful intelligence. The overall process begins with data input, followed by preprocessing, feature extraction, machine learning classification, and intelligence extraction. Initially, the user uploads a text file containing threat-related information through the web interface. This input may include threat reports, attack descriptions, or suspicious activity logs. Once the text is received, the preprocessing stage is applied to clean and normalize the data. This step removes punctuation, converts text into lowercase format, and eliminates unnecessary characters to ensure consistency. After preprocessing, the cleaned text is transformed into numerical features using the **Term Frequency–Inverse Document Frequency (TF-IDF)** technique. This method helps identify the importance of words in the document relative to the dataset. The TF-IDF representation allows the machine learning model to understand patterns within the textual data. The processed feature vectors are then provided to a trained classification model that predicts the most relevant threat category. Based on the predicted result, the system proceeds to extract additional intelligence indicators such as keywords related to phishing attempts, malware distribution, or system compromise. Finally, the system generates an automated summary explaining the identified threat category and the indicators found within the text. This output is displayed through the Streamlit interface, enabling users to quickly interpret the results.

VI. RESULTS AND DISCUSSION

The developed system successfully processes threat text inputs and predicts the corresponding threat category. The classification model was trained and evaluated using an augmented dataset containing multiple cyber threat categories. Experimental testing demonstrated that the system is capable of identifying threats such as phishing, malware, data breaches, and social engineering attacks.
In addition to classification, the system extracts threat indicators and generates a concise analytical summary of the detected threat. These results are displayed through the web dashboard, enabling users to quickly interpret the analysis results.

VII. SYSTEM ADVANTAGES

The ThreatSpeak system offers several advantages compared to traditional manual threat analysis methods. One of the main benefits is the **automation of threat classification**, which significantly reduces the time required to analyze textual threat reports. Security analysts can quickly obtain insights without manually reviewing large amounts of information. Another advantage is the **integration of machine learning with natural language processing**, allowing the system to analyze unstructured text effectively. This capability improves the accuracy and efficiency of threat detection compared to simple keyword-based approaches. The system also provides **automated threat intelligence extraction**, which highlights important indicators and targeted assets mentioned in the text. This feature helps users understand the context of the threat more clearly. In addition, the **web-based interface developed using Streamlit** makes the system easy to use. Users can upload files and obtain results without requiring advanced technical knowledge. The lightweight architecture of the application also ensures that it can run on standard computing environments without specialized infrastructure.

VIII. CONCLUSION AND FUTURE WORK

The ThreatSpeak system demonstrates how machine learning and natural language processing techniques can be applied to automate cyber threat intelligence analysis. The platform simplifies the process of analyzing threat reports by

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 2, February 2026
DOI: 10.17148/IJARCCE.2026.15248

automatically classifying the type of attack and extracting relevant information. The system provides a user friendly interface for uploading and analyzing threat data.

In the future, the system can be enhanced by integrating real time threat intelligence feeds and larger datasets for improved model accuracy. Additional features such as advanced NLP summarization, interactive dashboards, and database storage can further strengthen the capabilities of the platform.

REFERENCES

[1]. I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. MIT Press, 2016.
[2]. C. D. Manning, P. Raghavan, and H. Schütze, Introduction to Information Retrieval. Cambridge University Press, 2008.
[3]. National Institute of Standards and Technology, Guide to Cyber Threat Information Sharing, 2016.
[4]. European Union Agency for Cybersecurity, Cyber Threat Intelligence Overview, 2021.
[5]. OWASP Foundation, OWASP Top 10 Web Application Security Risks, 2021.

