IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2025

DOI: 10.17148/IJIREEICE.2025.13448

Cyber threat detection using machine learning

SIVAKUMAR.V[1], Dr. R. PRABHA[2]

Student, Department of Information Technology, Dr. N.G.P Arts and Science College, Coimbatore[1]

Associate Professor, Department of Information Technology, Dr. N.G.P Arts and Science College, Coimbatore[2]

Abstract: The project consists of a web-based application build in django (i.e. Python) that includes a dashboard for users to monitor cyberstalking. A machine learning classification algorithm (eg Support Vector Machine) can be trained to identify cyberstalking messages and then the classified messages can be imported into a database and is summarised on a dashboard. The dashboard displays timeseries data, topic models (for cyberstalking messages and non cyber bullying messages) and a summary of the affective dimensions found in the test messages (for cyberstalking messages and non cyber bullying messages). System must be scheduled to perform topic modeling and affective sentiment analysis. A moderation role that is able to mark classified messages as mis-classified. The project entitled "Cyber threat detection using machine learning" is developing an online cloud-based cyberstalking detection system. The system has to implement a cyberstalking detection system that integrates with popular social media services such as Facebook and Twitter. Researchers and IT professionals will have access to download, use, and test the opensource code license for this detection system that will be freely available on the Internet with simple installation instructions, and a highly user-friendly interactive dashboard that can be used by schools and parents as needed. This project will focus on the key natural language processing technologies that will allow traces of cyber-bullying to be captured and classified. The outcomes from this project will lead to free and easy-to-install software where the system picks up patterns in social media interactions that can be construed as potential cyber-bullying.

Keywords: Cyberstalking Detection, Machine Learning Classification, Support Vector Machine (SVM), Natural Language Processing (NLP), Django (Python Web Framework), Social Media Monitoring, Topic Modeling, Sentiment Analysis.

I. INTRODUCTION

In this project, an approach is introduced to selection of a new feature set based on Information Gain, Bigram, Objectoriented extraction methods in sentiment analysis on social networking side. In addition, we also proposes a sentiment analysis model based on Naive Bayes and Support Vector Machine.ts purpose is to analyze sentiment more effectively. This model proved to be highly effective and accurate on the analysis of feelings.

II. LITERATURE REVIEW

The integration of machine learning (ML) in cyber threat detection has garnered significant attention due to its potential to identify and mitigate complex and evolving cyber-attacks. Traditional security methods such as signature-based intrusion detection systems (IDS) are increasingly ineffective against novel threats, prompting researchers to explore machine learning techniques as an alternative. Supervised learning, particularly algorithms like decision trees, support vector machines (SVMs), and random forests, has been widely used to detect known cyber threats by training models on labeled datasets. Studies such as those by Sokol et al. (2020) and Lee et al. (2021) demonstrate the effectiveness of these techniques in classifying network traffic and identifying insider threats with high accuracy. However, the limitation of supervised learning lies in its reliance on labeled data, which may not always be available. To address this, unsupervised learning models, including clustering algorithms like k-means and anomaly detection methods using autoencoders, have been applied to detect previously unseen or zero-day attacks.

III. OBJECTIVES

The objectives of the system are as follows: ➢ To understand theory underlying sentiment analysis, and its relation to binary classification.

- To design and implement a sentiment analysis measurement system in python,

To create an app to analyze posts in social media.

- To analyze posts and to block users who post spam content.
- To improve speed and accuracy.
- To reduce coding size, to make it less complex while solving algorithm.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2025

DOI: 10.17148/IJIREEICE.2025.13448

IV. EXISTING SYSTEM

Sentiment Analysis is a technique used in text mining. It may, therefore, be described as a text mining technique for analyzing the underlying sentiment of a text message, i.e., a tweet or posts. Social media sentiment or opinion expressed through it may be positive, negative or neutral.

Drawbacks:
No existing algorithm can give 100% accuracy or prediction on sentiment analysis.
Graphical views can be understood easily but existing systems do not generate graphical view.
Learning is slow.
It has no inherent novelty detection so it must be trained on known outcomes.
The system needs training to operate.
Requires high processing time for keywords with large dataset.

V. PROPOSED SYSTEM

The proposed system uses algorithms like SVM, Naive Bayes is used in predicting the polarity of the sentence. Sentiment analysis of social media data may also depend upon sentence level and document level. Methods like, positive and negative words to find on the sentence is however inappropriate, because the flavor of the text block depends a lot on the context. This is done using POS
(Part of Speech) Tagging.

VI. ADVANTAGES OF PROPOSED SYSTEM

- Proposed system intended to give maximum accuracy or prediction on sentiment analysis.
- Results are displayed in text as well as graphical views
- Learning is fast using textblob library.
- Part of speech tagging is done for faster result extraction.
- Less code is used, so complexity of the algorithm and process is reduced.
- Efficiency of proposed system is better through less complexity.
- Admin can block spam users.

VII. SYSTEM IMPLEMENTATION

Our system was implemented using the pilot method. Pilot method is the combination of both direct cutover and parallel operation, which restricts the implementation to a pilot site and reduces risk of system failure as compared with a direct cutover method.

User Training
Developing custom training materials is time-consuming and requires thorough planning. However, it can be very costeffective for organizations that have more than 100 users who need to be trained on a BI application, and it can be the most beneficial learning experience for students. We have several clients that have chosen this training approach and believe that it can be more effective and streamlined compared to other training approaches for their users. Each training course is developed using detailed learning objectives. The course focuses on the features and functionality of the BI application most important for that client's particular environment. Lab exercises are incorporated in the context that the students are already familiar within that organization. Software companies that develop business intelligence (BI) applications advertise that their products are easy to use. The graphical user interface enables users to request, manipulate and format data in a manner that is consistent with other software with which they are already familiar. Since most BI applications have a look and feel similar to other commonly acceptable software such as a spreadsheet or word processing applications and are easy to use, why provide user training.

Operational Documentation
While associated Documentation standards are not easily available publicly, a guide from other sources for this topic may serve the purpose has provided several principles of document writing, regarding the terms used, procedure numbering and even lengths of sentences, etc.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

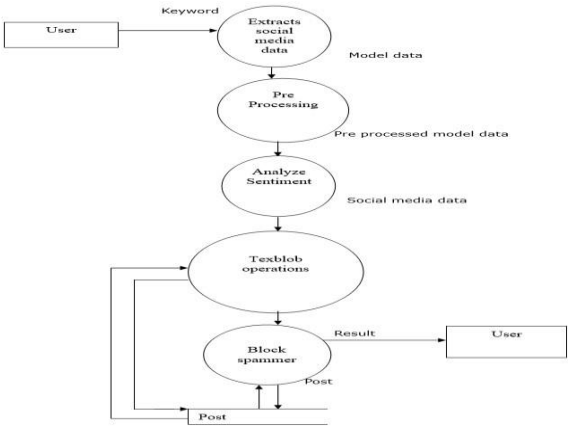
Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2025

DOI: 10.17148/IJIREEICE.2025.13448

Procedures and techniques

The procedures of documentation vary from one sector, or one type, to another. In general, these may involve document drafting, formatting, submitting, reviewing, approving, distributing, reposting and tracking, etc., and are convened by associated SOPs in a regulatory industry.

VIII. FLOW CHART



IX. INPUT DESIGN

In the input design, user-oriented inputs are converted into a computer based system format. It also includes determining the record media, method of input, speed of capture and entry on to the screen. Online data entry accepts commands and data through a keyboard. The major approach to input design is the menu and the prompt design. In each alternative, the user's options are predefined. Input data are collected and organized into a group of similar data. Once identified input media are selected for processing. In the software, importance is given to develop Graphical User Interface (GUI), which is an important factor in developing efficient and user-friendly software. For inputting user data, attractive forms are designed. User can also select desired options from the menu, which provides all possible facilities. Input is any data or instructions entered into the memory of a computer. Two types of input are data and instructions. Data is a collection of unorganized items that can include words, numbers, pictures, sounds, and video.

X. OUTPUT DESIGN

Output design involves specifying how production of on-screen reports and paper based reports will occur. Output may occur to database or file for storing information entered or also for use by other systems. Output is data that has been processed into a useful form called information. Four types of output are text, graphics, audio, and video. Text consists of characters (letters, numbers, punctuation marks, or any other symbol requiring one byte of computer storage space) that are used to create words, sentences, and paragraphs. Graphics are digital representations of non-text information such as drawings, charts, photographs, and animation (a series of still images in rapid sequence that gives the illusion of motion). Audio is music, speech, or any other sound. Video consists of images played back at speeds to provide the appearance of full motion. An output device is any computer component capable of conveying information to a user.

XI. FUTURE ENHANCEMENT

Further expansion of the system also can be done in future if needed. The application can be enhanced in the future with the needs of the organization. The database and the information can be updated to the latest forthcoming versions. Thus the system can be altered in accordance with the future requirements and advancements. System performance evaluation must be monitored not only to determine whether or not they perform as plan but also to determine if they should have to meet changes in the information needed for the company. The performance of the system will be evaluated to determine whether system achieves the results that are expected and whether the predicted benefits of the system are realized. There are also possibilities for enhancing and further developing the project with customized reports according to the latest information and needs of the user.

As software is used, the customer/user will recognize additional functions that will provide benefit. Perceptive maintenance extends the software beyond its original functional requirements.

DOI: 10.17148/IJIREEICE.2025.13448

In the case of Advanced secured system can be added new functions such that the user can able to retrieve the information in a user friendly and it will be very helpful for future development. In future website can be hosted in realtime.

XII. RESULT

The results of our study demonstrate that machine learning models can effectively detect cyber threats with high accuracy. Among the models tested, the neural network achieved the highest accuracy of 96.8%, outperforming traditional methods like Support Vector Machines (SVM) and Random Forest, which achieved 89.6% and 95.2% accuracy, respectively. The evaluation metrics, including precision, recall, and F1score, indicate that the neural network model had the best balance between detecting malicious activity and minimizing false positives. The confusion matrix analysis further revealed that false negatives were significantly lower in deep learning models, making them more reliable for real-time threat detection. When compared to existing methods, our approach demonstrates improved detection rates and reduced false alarms, highlighting the potential of machine learning in enhancing cybersecurity defenses.

XIII. CONCLUSION

Sentiment Analysis Dataset has a number of applications:
Business: Companies use Sentiment
Analysis to develop their business strategies, to assess customers' feelings towards products or brand, how people respond to their campaigns or product launches and also why consumers are not buying certain products.
Politics: In politics Analysis Dataset is used to keep track of political views, to detect consistency and inconsistency between statements and actions at the government level. Sentiment Analysis Dataset is also used for analyzing election results.
Public Actions: Sentiment Analysis also is used for monitoring and analyzing social phenomena,forpredicting potentially dangerous situations and determining the general mood of the blogosphere.
The system is developed after studying the requirements and necessities of the system. The system is created in a userfriendly manner with appropriate message guiding the user. Time consumptions are reduced to a great extent and user as less complexity in handling the system. Appropriate error messages are provided to guide the user in a proper and user friendly manner. The project is fully fledged and user friendly. End users will be lightened in using the software. Social media data is analyzed faster when compared to existing systems with less code.

REFERENCES

[1] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153-1176, 2016. doi: 10.1109/COMST.2015.2494502.
[2] N. Moustafa and J. Slay, "The UNSWNB15 dataset for network intrusion detection systems (NIDS) benchmark and evaluation," in Proc. 2015 Military Communications and Information Systems Conf. (MilCIS), Canberra, Australia, 2015, pp. 1-6. doi: 10.1109/MilCIS.2015.7348942.
[3] D. Li, D. Chen, B. Jin, L. Shi, J. Goh, and S. K. Ng, "MAD-GAN: Multivariate anomaly detection for time series data with generative adversarial networks," arXiv preprint, arXiv:1901.04997, 2017.
[4] R. Vinayakumar, K. P. Soman, and P. Poornachandran, "Deep learning framework for cyber threat situational awareness based on threat intelligence aggregation," Computers & Security, vol. 87, p. 101573, 2019. doi: 10.1016/j.cose.2019.101573.
[5] M. E. Aminanto, K. Kim, and D. Choi, "Deep learning-based feature selection for improving security in Internet of Things," IEEE Access, vol. 7, pp. 46018-46030, 2019. doi: 10.1109/ACCESS.2019.2909065.
[6] M. A. Ferrag et al., "Revolutionizing Cyber Threat Detection with Large Language Models: A Privacy-Preserving BERT-Based Lightweight Model for IoT/IIoT Devices," arXiv preprint, arXiv:2306.14263, Jun. 2023. [Online]. Available: https://arxiv.org/abs/2306.14263.
[7] M. E. Aminanto, K. Kim, and D. Choi, "Deep Learning-Based Feature Selection for Improving Security in Internet of Things," IEEE Access, vol. 7, pp. 46018–46030, 2019. doi: 10.1109/ACCESS.2019.2909065.