Research Article

DETECTING AND CLASSIFYING FRAUDULENT SMS AND EMAIL WITH A ROBUST MACHINE LEARNING APPROACH

Dr. P. BUJJI BABU[1] TANGIRALA NAGA ASWINI[2] MURARISETTY HOMA SRI VISHNU[3] BATTULA GOPIPRASHANTH[4] BALA SUDARSAN REDDYJANAPALA[5]

[1]Department of CSE & AI, Chalapathi Institute of Engineering and Technology, LAM, Guntur, Andhra Pradesh, India.
[2]Department of CSE & AI, Chalapathi Institute of Engineering and Technology, LAM, Guntur, Andhra Pradesh, India.
[3]Department of CSE & AI, Chalapathi Institute of Engineering and Technology, LAM, Guntur, Andhra Pradesh, India.
[4]Department of CSE & AI, Chalapathi Institute of Engineering and Technology, LAM, Guntur, Andhra Pradesh, India.
[5]Department of CSE & AI, Chalapathi Institute of Engineering and Technology, LAM, Guntur, Andhra Pradesh, India

Abstract: Spam is an unwanted message or SMS sent onmobile phones whose content may bemalicious. Scammers sendfake text messages to trick people into responding to their SMSand they may hack personal information, password, accountnumber, etc. To avoid being tricked by scammers, proposed amodel based on Machine learning Algorithms. The proposedmodel is implemented using the Naïve Bayes algorithm and termfrequency-inverse document frequency vectorizer. Obtainedthe dataset from Kaggle and trained the model using it. Thismodel consists of a local host website which is obtained throughPyCharm IDE. Obtained results show that the model accuracyof 95% and a precision of 100%.

Key words: Spam SMS, Spam Email, Machine Learning, Naïve Bayes, Cyber Crime, Cyber Scam

1.INTRODUCTION

whole world is moving towards digitalization. Peopleconverse, send money and do many activities which make lifeeasier. Even though it has many pros it also has many constoo. Nowadays people are targeted by online scammers andget tricked easily. People may receive suspicious links, unrecognized contact numbers, offers, etc. through emails,SMS, and social media. The messages can be receivedrandomly or targeted on particulars. Sometimes the messagesmight seem to be non-spam which can trick people and canget successful in scamming. Online scams come undercybercrime and the thief can be sentenced to punishments butdue to a lack of awareness in the general public, these crimescan go unnoticed which may promote these scam activitiesmore. Cybercrime offices, telecom companies, and bankswarn people about spammers and hackers who trick peopleby sending messages, links, and emails. But normally peopleare not aware of whether the messages and emails they getare verified or fake due to this reason cyber scamshappen [19]. A private firm named Local Circles conducted asurvey in which the statistics showed that in the last 3 years42% of Indians faced financial fraud and 74% of people failedto retrieve the money. To overcome these cyber scams, proposed a model based on machine learning which helpsindividuals to check if the messages and emails they arereceiving are spam or not. Whenever the user feels themessage is unsafe, they can copy and paste it into the opensourcesite created.

2.LITERATURE SURVEY

Lutfun Nahar Lota et al. [1] explained how SMS spam detection can be more challenging compared to other types of detection. Different algorithms that can be used and the scope of improvisation. Through this paper, able to study many more literature reviews on the same topic. Paras Sethi et al. [2] explained how big of a problem SMS spam is globally. different algorithms available for analyzing the model and which ones can be the best among them and also studied different filtering methods. Shafi'i muhammadabdulhamid et al. [3] summarized a review of the methods that are generally used, probable challenges that can occur, and the scope for future research on spam filtering and spam detection in mobile SMS. This paper provided the details on available filtering techniques that can be used in the model to check different parameters like accuracy.

3.SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

The existing system for your project "Spam SMS (or) Email Detection and Classification using Machine Learning" is designed to tackle the issue of identifying and categorizing spam SMS messages to protect users from potentially harmful content and fraudulent activities. It employs the Naïve Bayes algorithm for classification and a term frequency-inverse document frequency (TF-IDF) vectorizer for feature engineering. The project utilizes a dataset obtained from

Kaggle for training the model. The system includes a user-friendly interface in the form of a local host website, which allows users to input SMS messages and receive the classification results. Based on the abstract, the system has demonstrated strong performance with a 95% accuracy rate and a precision of 100%, indicating a high level of accuracy in correctly identifying spam messages and minimizing false positives.

LIMITATIONS OF EXISTING SYSTEM

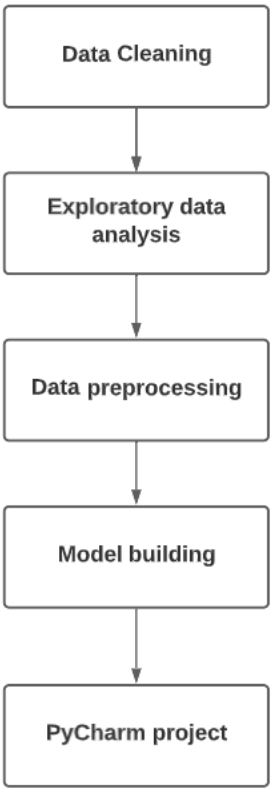
Adversarial Attacks: There's a growing concern about adversarial attacks against ML models, where attackers deliberately craft messages to exploit weaknesses in the model.

Privacy Concerns: The use of ML in screening emails and SMS for fraud detection raises significant privacy concerns.

3.2 PROPOSED SYSTEM

The major steps in the process are data cleaning, exploratory data analysis, data preprocessing, model building, and the PyCharm IDE. system architecture shows the detailed flowchart of spam SMS detection. Initially, the dataset is separated as spam and ham. Spam is assigned with 1 and ham is assigned with 0. Each SMS from the dataset breaks into a number of characters, words, and sentences and then be analyzed. The data converted to lowercase, tokenized, and stemming will be applied. Using Naïve Bayes algorithms, it is vectorized. Hence, this leads to the completion of model building. utilizes machine learning techniques such as Naïve Bayes and TF-IDF vectorization to improve accuracy in detecting and classifying spam SMS or emails. By training on a Kaggle dataset and implementing within a local host website, it aims to achieve high effectiveness in safeguarding users against spam messages.

4. SYSTEM ARCHITECTURE



5.MODULES

Data Collection and Preprocessing Module: This module is responsible for collecting data from various sources, such as SMS messages, multimedia messages, and emails. It preprocesses the data, including text normalization, removal of noise, and feature extraction. It ensures that the data is ready for analysis and classification.
Machine Learning Model Module: This module involves the implementation of machine learning models for spam detection and classification. It encompasses model training, validation, and evaluation. The module can include a variety of models, including Naïve Bayes, deep learning, and ensemble methods.

Real-Time Threat Intelligence Module: To stay updated with emerging spam tactics, this module continuously monitors and collects data from real-time threat intelligence sources, external APIs, and user-generated reports. It incorporates this information into the system to enhance its accuracy and effectiveness.

User Interface and Reporting Module: This module provides a user-friendly interface for users to interact with the system. Users can input messages, view classification results, and report false positives or negatives. It also generates reports and visualizations to convey the system's performance to users.

Scalability and Deployment Module: To ensure that the system can handle increased user demand and message volume, this module focuses on scalability and cloud deployment. It manages system resources, load balancing, and scalability mechanisms to ensure a seamless user experience.

6.RESULT

7.CONCLUSION

The danger of spam SMS is increasing all over the world at a very high rate and keeps on accelerating since access to the internet and mobile connectivity has increased. India is getting higher exposure to this phenomenon because of the availability of SMS services at lower cost. As a matter of precaution and to avoid fraud occurrences the model proposes a machine learning-based solution. The presented spam SMS filtering method is analyzed based on various algorithms, visualized through graphs and charts, and finally based on performance, accuracy, and precision; it implements TF-IDF with the Naïve Bayes classification. The proposed model is a user interface consisting of a block to write a message and a prediction button that informs whether the message is spam or not. This makes the model easy to use and adaptable for all age groups of people. As this model gives better accuracy and precision.

Future scope In totality, this research serves as a testament to the necessity of continuous vigilance in the realm of spam detection and computer forensics. By dissecting the intricacies of browser data storage and evaluating the performance of diverse algorithms, this study contributes to the evolving landscape of digital security, enriching the toolkit of professionals tasked with safeguarding digital communications and thwarting cyber threats.

REFERENCES

[1] Lutfun Nahar Lota et al. “A Systematic Literature Review on SMSSpam Detection Techniques”, I.J. Information Technology andComputer Science, 2017, 7, 42-50.
[2] P. Sethi et al. “SMS spam detection and comparison of variousmachine learning algorithms,” International Conference on Computingand Communication Technologies for Smart Nation (IC3TSN), 2017,pp. 28-31.
[3] S. M. Abdulhamid et al. “A Review on Mobile SMS Spam Filtering Techniques,” IEEE Access, vol. 5, pp. 15650-15666, 2017.

[4] M.Rubin Julis et al. “Spam Detection in SMS Using Machine Learning Through Text Mining”, International journal of scientific & technology research, vol 9, Issue 02, 2020.
[5] A. Alzahrani et al. “Comparative Study of Machine Learning Algorithms for SMS Spam Detection,” SoutheastCon, 2019, pp. 1-6.
[6] N. Nisar et al. “Voting-Ensemble Classification for Email Spam Detection,” International Conference on Communication information and Computing Technology (ICCICT), 2021, pp. 1-6.
[7] S. Agarwal et al. “SMS spam detection for Indian messages,” International Conference on Next Generation Computing Technologies (NGCT), 2015, pp. 634-
[8] Michael Crawford et al. “Survey of Review spam detection using machine learning techniques”, Journal of Big Data, 2015.
[9] Anju Radhakrishnan et al. “Email Classification using Machine learning algorithms”, International Journal of Engineering and Technology (IJET), 2017.pp.335-340.
[10] N. Govil et al. “A Machine Learning based Spam Detection Mechanism,” International Conference on Computing Methodologies and Communication (ICCMC), 2020, pp. 954-957. [11] Shirani-Mehr et al. “SMS spam detection using machine learning approach” 2013,1-4.