Real Time Spam Mail Deriation Expert System Using NLP and Neural Networks

Mr.G.BalaMurugan[1], Mr.M.Sabari Ramachandran[2], J. Uvaiskhan[3]
[1,2,3]*Department of MCA, MohamedSathak Engineering, College, Kilakarai, India*

Abstract- Email has become an integral part of communication in today's world, playing a crucial role in both personal and professional domains. It provides a quick and convenient way to exchange information, documents, and messages globally. The surge in cybersecurity incidents has witnessed attackers increasingly exploiting sophisticated spam emails as a gateway to breach government systems, major corporations, and the online platforms of public figures and organizations worldwide. While the public eye is keenly focused on detecting spam within vast email datasets, the challenge has escalated due to the growing complexity of camouflage techniques employed by cybercriminals. Existing detection methods struggle to keep pace with the intricate deception methods and the sheer volume of emails, emphasizing the urgent need for innovative and adaptive approaches, including advanced machine learning, behavioural analysis, and collaborative threat intelligence sharing, to fortify our defences against evolving cyber threats. In this project, we proposed to design a novel efficient approach named E-Mail Screener for big e-mail data classification into four different classes: Normal, Fraudulent, Harassment, and Suspicious E-mails by using NLP and BiLSTM. The new method includes two important stages, sample expansion stage and testing stage under sufficient samples. This project The NLP and BiLSTM efficiently captures meaningful information from E-mails that can be used for forensic analysis as evidence. Experimental results revealed that E-Mail Screener performed better than existing ML algorithms and achieved a classification accuracy of 99.1% using the novel technique of BiLSTM with recurrent gradient units. As different types of topics are discussed in E-mail content analysis. E-Mail Screener effectively outperforms existing methods while keeping the classification process robust and reliable.

Keywords- E-Mail Screener, NLP and BiLSTM.

1. INTRODUCTION

Email stands for Electronic Mail. It is a method to sends messages from one computer to another computer through the internet. It is mostly used in business, education, technical communication, document interactions. It allows communicating with people all over the world without bothering them. In 1971, a test email sent Ray Tomlinson to himself containing text.

Figure 1: E-Mail

Email messages are conveyed through email servers; it uses multiple protocols within the TCP/IP suite. For example, SMTP is a protocol, stands for simple mail transfer protocol and used to send messages whereas other protocols IMAP or POP are used to retrieve messages from a mail server. If you want to login to your mail account, you just need to enter a valid email address, password, and the mail servers used to send and receive messages.

Although most of the webmail servers automatically configure your mail account, therefore, you only required to enter your email address and password. However, you may need to manually configure each account if you use an email client like Microsoft Outlook or Apple Mail. In addition, to enter the email address and password, you may also need to enter incoming and outgoing mail servers and the correct port numbers for each one.

Email messages include three components, which are as follows:

- Message envelope: It depicts the email's electronic format.
- Message header: It contains email subject line and sender/recipient information.
- Message body: It comprises images, text, and other file attachments.

2. RELATED WORKS

E-mail is an essential application for carrying out transactions and efficiency in business processes to improve productivity. E-mail is frequently used as a vital medium of communication and is also being used by cybercriminals to commit crimes. Cybercrimes like hacking, spoofing, phishing, E-mail bombing, whaling, and spamming are being performed through E-mails. Hence, there is a need for proactive data analysis to prevent cyber-attacks and crimes. To investigate crimes involving Electronic Mail (e-mail), analysis of both the header and the email body is required since the semantics of communication helps to identify the source of potential evidence. With the continued growth of data shared via emails, investigators now face the daunting challenge of extracting the required semantic information from the bulks of emails, thereby causing a delay in the investigation process. The existing email classification approaches lead towards irrelevant E-mails and/or loss of valuable information.

3. PROPOSED WORKS

The The proposed approach comprises data collection, pre-processing, feature extraction, parameter tuning, and classification using the LSTM-GRU model. In this project, E-mail datasets are divided into normal, harassing, suspicious, and fraudulent classes. The E-mail is divided into word levels of the E-mail body, and the embedding layer is applied to train and obtain the sequence of vectors.

LSTM and GRU

In Deep learning, Long-Term Short-Term Memory Networks and Gated Recurrent Units, LSTM and GRUs for short.

LSTM – Long Short-Term Memory

LSTMS are a special kind of RNN which is capable of learning long-term dependencies. LSTMs are designed to dodge long-term dependency problem as they are capable of remembering information for longer periods of time. Long short-term memory (LSTM) units (or blocks) are a building unit for layers of a recurrent neural network (RNN). A RNN composed of LSTM units is often called an LSTM network. A common LSTM unit is composed of a cell, an input gate, an output gate and a forget gate. The cell is responsible for "remembering" values over arbitrary time intervals; hence the word memory" in LSTM. Each of the three gates can be thought of as a "conventional" artificial neuron, as in a multi-layer (or feedforward) neural network: that is, they compute an activation (using an activation function) of a weighted sum. Intuitively, they can be thought as regulators of the flow of values that goes through the connections of the LSTM; hence the denotation "gate". There are connections between these gates and the cell. The expression long short-term refers to the fact that LSTM is a model for the short-term memory which can last for a long period of time. An LSTM is well-suited to classify, process and predict time series given time lags of unknown size and duration between important events. LSTMs were developed to deal with the exploding and vanishing gradient problem when training traditional RNNs.

System architecture:

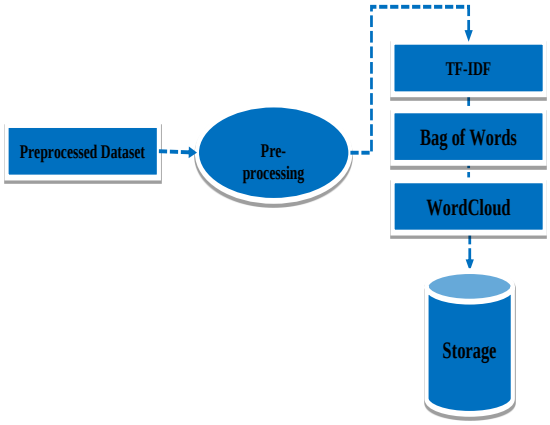

Figure 2: System architecture

Algorithm:

•Support vector machine

SVM are based on the assumption that the input data can be linearly separable in a geometric space. This is often not the case when working with real word data. To solve this problem SVM map the input to a high dimension feature space, i.e hyperplane, where a linear decision boundary is constructed in such a manner that the boundary maximises the margin between two classes. SVM is introduced as a binary classifier intended to separate two classes when obtaining the optimal hyperplane and decision boundary.

•Decision tree

A DT classifier is modelled as a tree where rules are learned from the data in a if-else form. Each rule is a

node in the tree and each leaf is a class that will be assigned to the instance that fulfil all the above nodes conditions. For each leaf a decision chain can be created that often is easy to interpret. The interpretability is one of the strengths of the DT since it increases the understanding of why the classifier made a decision, which can be difficult to achieve with other classifiers. The telecommunication company is today using a manually created decision tree, in which the rules are based on different combinations of words.

•Naive bayes

The NB classifier is considered to perform optimal when the features are independent of each other, and close to optimal when the features are slightly dependant. Real world data does often not meet this criterion but researchers have shown that NB perform better or similar to C4.5, a decision tree algorithm in some settings. The researchers argue that NB performs well even when there is a clear dependency between the features, making it applicable in a wide range of tasks.

•AdaBoost

ADA is built upon the premise that multiple weak learners that perform somewhat good can be combined using boosting to achieve better result. This algorithm performs two important steps when training and combining the weak classifiers, first it decided which training instances each weak classifier should be trained on, and then it decides the weight in the vote each classifier should have. Each weak classifier is given a subset of the training data that where each instance in the training data is given a probability that is decided by the previous weak classifiers performance on that instance. If the previous weak classifiers have failed to classify the instance correct it will have a higher probability to be included in the following training data set. The weight used in the voting is decided by each classifiers ability to correctly classify instances. A weak classifier that performs well is given more influence than a classifier that perform bad.

4. TESTING AND IMPLEMENTATION

Testing an email screener involves various methodologies to ensure its effectiveness, accuracy, and reliability.

Testing Methodology

1. Planning and Preparation

Outline what you aim to achieve with the testing. Create a detailed plan that includes test cases, resources needed, timelines, and responsibilities. Ensure the environment mimics production as closely as possible.

2. Functional Testing

Test individual components like filters and rules to verify they work correctly in isolation. Assess how well the screener integrates with other systems (e.g., email servers, databases). Verify that the entire system works as expected in a complete environment.

3. Performance Testing

Evaluate the screener's performance under expected email volumes. Determine how the screener performs under extreme conditions or high loads. Test if the screener can handle increasing amounts of data or traffic.

4. Security Testing

Identify and address potential security weaknesses. Simulate attacks to discover vulnerabilities. Ensure the screener adheres to relevant data protection and privacy regulations (e.g., GDPR, HIPAA).

5. Usability Testing

Check the design and layout for usability and user-friendliness. Collect feedback from actual users about their experience with the screener.

6. Accuracy Testing

Measure the rate of incorrect classifications (e.g., legitimate emails marked as spam). Evaluate how well the screening rules and filters perform in practice.

7. Compatibility Testing

Ensure the screener works across different email clients, operating systems, and devices. Verify that the screener is compatible with various web browsers if applicable.

8. Regression Testing

Use automated tools to re-run previous test cases to ensure new changes haven't introduced new issues. functions.

Implementation

1. Email Screener Web App

Build an E-mail Forensics Predictor service is an online platform which people use emails free from spam. In this module we developed the Web based GUI is developed for the email classification system to categorize the email as spam or not spam. Integrate

with Trainer and Tester Modules Developed with Python and Flask Framework.

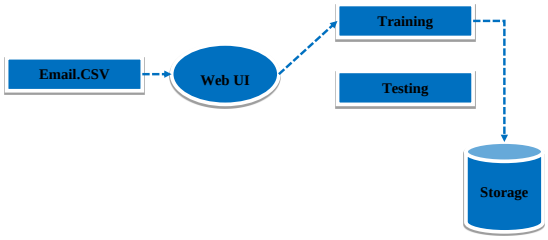

Figure 3: Email Screener Web App

2. E-Mail Classification – Training Phase
Dataset Annotation
In this project, E-mails are divided into normal, harassing, suspicious, and fraudulent classes. The E-mail is divided into word levels of the E-mail body, and the embedding layer is applied to train and obtain the sequence of vectors.
E-mail Data Set Preparation and Exploration
Import Dataset
In this module the admin uploads an email dataset (CSV) file. This will be used to train your email forensics analysis model.
Read Dataset
The EmailSinkAI reads email dataset to output the purpose or objective of the project.
Explore Dataset – EDA
Data visualization tool that brings the entirety of data together into a striking and easy-to-follow view.
Data Pre-processing
The data pre-processing phase consists of natural language-based steps that standardize the text and prepare it for analysis.
Feature Extraction
After eliminating irrelevant information, the elaborated list of words is converted into numbers. The TF-IDF method is applied to accomplish this task.

LSTM based GRU Classification Model
LSTM comprises the classification of E-mails as Normal, Harassing, Suspicious, and Fraudulent.

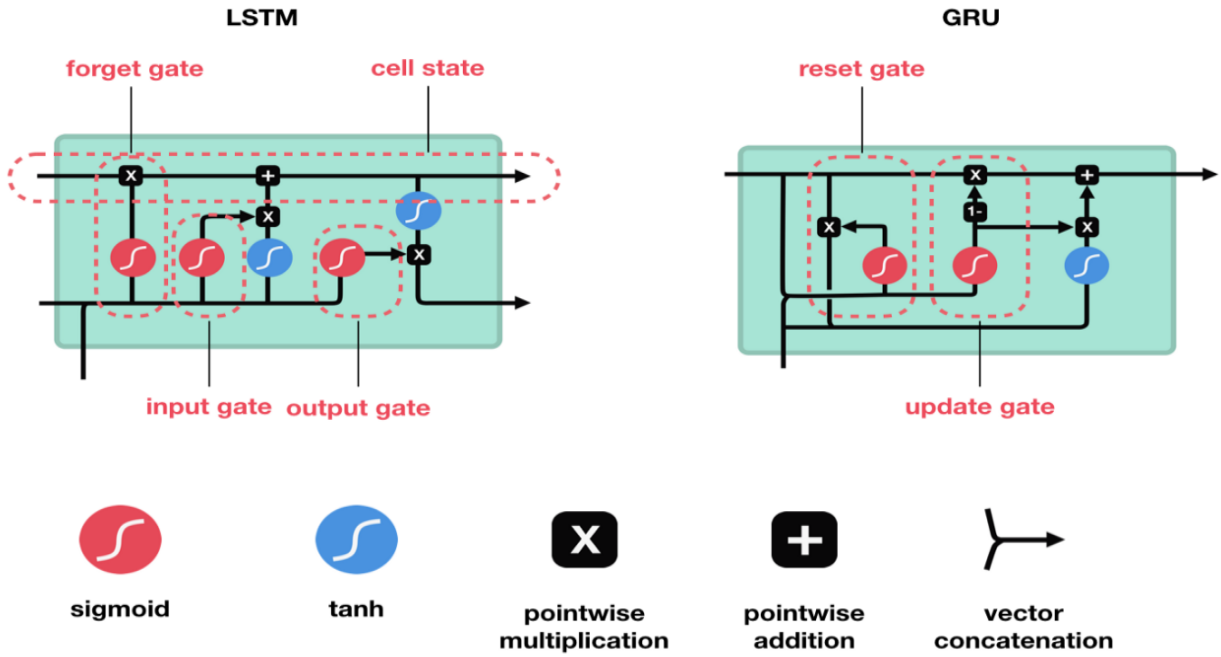

Figure 4: E-Mail Classification – Training Phase

3. E-Mail Forensic Analyser – Testing Phase
Email Account Integrator
In this module, user register here and login with their username and password and input their email ID and email Password to filter spam.
Read Mail
This module reads the new mails
Extract Feature
Extract spam feature from the new mails
E-Mail Forensic Predictor
This module predicts whether it is spam or not spam and classify the type.

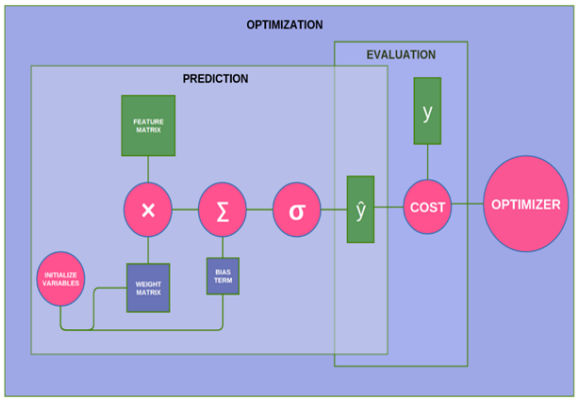

Figure 5: E-Mail Forensic Analyser – Testing Phase

5. CONCLUSION AND FUTURE ENHANCEMENTS

Conclusion

This project proposed a LSTM model with an embedding layer for multiclass classification of electronic mails. We evaluated the proposed Email Gateway model using evaluation metrics such as precision, recall, accuracy, and f-score. Experimental results revealed that Email Gateway performed better than existing ML algorithms and achieved a classification accuracy of 95% using the novel technique of LSTM with recurrent gradient units.

Future enhancement

In envisioning the future enhancements of our educational management system, we are eager to incorporate virtual and augmented reality elements. This innovation aims to redefine the learning experience by introducing immersive features such as virtual labs and simulations. Students will have the opportunity to engage dynamically with intricate concepts, fostering a deeper understanding through interactive exploration. Additionally, our system's integration with Learning Management Systems (LMS) is a strategic move towards a more streamlined educational ecosystem. Whether through collaboration with existing LMS or the development of an integrated module, this initiative seeks to provide educators with a centralized platform for seamless course management, content delivery, and assessment. These advancements represent a commitment to creating a technologically enriched and cohesive learning environment for both students and educators.

REFERENCE

[1] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, ``A comprehensive survey of AI-enabled phishing attacks detection techniques,'' Telecommun. Syst., pp. 116, Oct. 2020.

[2] C. Iwendi, Z. Jalil, A. R. Javed, T. Reddy, R. Kaluri, G. Srivastava, and O. Jo, ``KeySplitWatermark: Zero watermarking algorithm for software protection against cyber-attacks," IEEE Access, vol. 8, pp. 7265072660, 2020.

[3] A. Rehman, S. U. Rehman, M. Khan, M. Alazab, and T. Reddy, ``CANintelliIDS: Detecting in-vehicle intrusion attacks on a controller area network using CNN and attention-based GRU," IEEE Trans. Netw. Sci. Eng., early access, Feb. 19, 2021, doi: 10.1109/TNSE.2021.3059881.

[4] S. U. Rehman, M. Khaliq, S. I. Imtiaz, A. Rasool, M. Shaq, A. R. Javed, Z. Jalil, and A. K. Bashir, ``DIDDOS: An approach for detection and identication of distributed denial of service (DDoS) cyberattacks using gated recurrent units (GRU)," Future Gener. Comput. Syst., vol. 118, pp. 453466, May 2021.

[5] S. I. Imtiaz, S. U. Rehman, A. R. Javed, Z. Jalil, X. Liu, and W. S. Alnumay, ``DeepAMD: Detection and identification of Android malware using high efficient deep artificial neural network," Future Gener. Comput. Syst., vol. 115, pp. 844856, Feb. 2021.