Detection of Email Spam using Natural Language Processing Based Random Forest Approach

Alanazi Rayan (alanaziphd2021@gmail.com)
Jouf University

Ahmed I. Taloba
Assiut University

Research Article

Keywords: Email, Spam, Temporal email, Natural Language Processing, Random Forest

Posted Date: September 27th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-921426/v1

Detection of Email Spam using Natural Language Processing Based Random Forest Approach

Alanazi Rayan[1], Ahmed I. Taloba[1a]
[1]Department of Computer Science, College of Science & Arts, Jouf University, Saudi Arabia. alanzirayanjouf@gmail.com
[a] Information System Department, Faculty of Computers and Information, Assiut University, Egypt.

alanaziphd2021@gmail.com

Abstract— **An unsolicited means of digital communications in the internet world is the spam email, which could be sent to an individual or a group of individuals or a company. These spam emails may cause serious threat to the user i.e., the email addresses used for any online registrations may be collected by the malignant third parties (spammers) and they expose the genuine user to various kinds of attacks. Another method of spamming is by creating a temporary email register and receive emails that can be terminated after some certain amount of time. This method is well suited for misusing those temporary email addresses for sending free spam emails without revealing the spammers real account details. These attacks create major problems like theft of user credentials, lack of storage, etc. Hence it is essential to introduce an efficient detection mechanismthrough feature extraction and classification for detecting spam emails and temporary email addresses. This can be accomplished through a novel Natural Language Processing based Random Forest (NLP-RF) approach. With the help of our proposed approach, the spam emails are reduced and this method improves the accuracy of spam email filtering, since the use of NLP makes the system to detect the natural languages spoken by people and the Random Forest approach uses multiple decision trees and uses a random node for filtering the spams.**

Keywords— Email, Spam,Temporal email,Natural Language Processing,Random Forest

I. INTRODUCTION

Nowadays, the spamming activity is rapidly spreading in various digital communication channels. The most widespread distribution of spam occurs through emails. Spammers mainly propagate spam emails for advertisement and create more mischievous actions including economic disruption and defamation in both personal as well as official life. The present strategies utilized for distinguishing the emails have the difficulty of detecting the “zero days” attack, which may result in higher false positives rate (FPR), and less accuracy in detection. SPAM recognition using ANN may prone to error in their outputs as they include all the spam features at the training phase. In the DNS based techniques for spamming botnet detection, the effort of DNS features utilization is lacking for detecting spam sending bots. To solve this issue, several frameworks like spam filtering mechanisms, DNS based techniques etc. are introduced for detecting the spam. Yet, those methods are less effective since it takes more time for identifying the spam emails, more memory consumption, and also causes detection error at the output. Thus, a novel approach is introduced for feature selection and classification.

Phishing is generally a technique of network theft, in which the attacker aims to steal the personal or private information of a user by creating a fake website or a fake page which resembles the same as that of the original authenticated page. These websites are deployed by the attacker for people’s use to enter the personal or account details. This network threat is most commonly done by sending malicious links via e-mails or by sending banners and pop-ups which can be clicked without the conscious of the user and hence they could get trapped. Phishing is classified as Spear phishing, in which an individual or a group of individuals are targeted for phishing attack, Clone phishing, in which a clone of an existing email with a malicious link is sent to any of the users, since the target is only stealing the credential of everyone, and not for a specific person, Whaling, in which the higher level or senior executives like CEO of an organization are targeted for phishing attack [1].Abuse of Online Social Networks (OSN) is found frequently in news, like Facebook Cambridge Analytica crisis and bot-based election manipulation in Twitter. The media are only involved recently in abuse of OSN, but it has been happening a long decade. This abuse includes the opinion manipulation, spam advertisements for popularity, malware distribution and phishing. This spam and phishing attacks are often undergone by fake online accounts. Now-a-days, in Twitter, around 500 million tweets cannot be monitored and filtered manually. Hence, it is important to deploy a machine learning filtering system of fake and spam posts [2].Today’s world, internet is a crucial part in everyone’s life. But there has been a dark side in it, like fake medical pages, illegal webpages, gambling sites, etc. Even though there are several techniques to detect malicious webpages, the growth of those websites is not yet controlled. The contents of these websites are harmful for many of the users especially for children and youngsters.The machine learning based methods are popular nowadays for examining the contents of a webpage.Because of getting lot of profits, the spam websites use various internet spams to escape regulation. Thus, it is important to summarize the common spam techniques to solve this serious threat from malicious internet sites [3].

The spam emails are increasing from last decade and it is a great misfortune for internet, since it occupies storage unwantedly, and wastes the time and speed for sending messages. Automatic spam filtering is the common method of spam detection. But recently, spammers can easily bypass this technique.Traditionally, the spam emails are only blocked manually. But due to recent advancements like machine learning, these mails can be automatically filtered based on text analysis, black and white lists of domain names and community-primarily based methods. The text analysis is the most common approach for junk email filtering, based on Naïve Bayes approach, which expressly blocks all the electronic mails. Every individual or organization is very much concerned about the legitimate emails. They no need of blocking or rejecting the genuine emails, hence this method is not much efficient. The white list approach is based on allowing all the emails from open and white listed domain addresses and gives less importance to the mails from other that the listed addresses. It only delivers the mails after getting an acknowledgement from junk mail filtering system [4].Artificial intelligence and communication networks are observed to be in great progress in past decade. Cyberspace is also grown to be a most vital part in human life. Therefore, it is important for cyberspace security for social and economic stability. Online spamming is the major criteria for violating cyberspace security most commonly in Internet of Things based social media applications. The goal of a spammer is to transfer a spam message to various media to satisfy their needs in political or commercial fields.For a secure online environment, detecting spams are much important, especially in social media, in which the social and financial relationships should be analyzed and in semantic fields, because it is well known that public opinion is the main cause for the rise and fall of a product or service [5].In today's world, people are given enough rights to share their thoughts in internet. Their opinions on a particular service or a product are called the reviews. These reviews are the important tool for the success or failure of a product/service. Every organization and consumer thus relies on the reviews of a particular one. The positive review makes a product to reach better and increases the financial growth, whereas the negative reviews make a product to get failure. Thus, some organizations invest money to provide false or fake positive reviews for their own products to grow their business and attain much gain, and false negative reviews for their competitor products, which leads to loss for them. This shows that the reviewing system can change the whole marketing outcome. Thus, it is highly important to detect such spam reviews and ensure trustworthiness in the field of e-commerce [6].

Spam emails are recently causing several troubles in online world. Spam emails are waste of storage, time and bandwidth. According to recent statistical analysis, around 40% are spam emails i.e., 15.4 billion email per day and costs $355 million per year for the users. The only solution for this issue is the automatic email filtering method for filtering out the spam emails effectively. There exists a heavy competition between the spammers and spam filter methods. A long year back, the spam emails are blocked by filtering mails from some certain addresses or by some specific subject lines. But nowadays, the spammers use tricky methods like using random words in the beginning and end of the mail contents or by using random addresses. Machine learning and knowledge engineering are the two technologies for detecting spam emails and filter them. By using knowledge engineering, it is needed to create a set of rules for filtering whether the emails are spam or ham. These rules are framed by the users or the spam filtering tool developers.But this method is not much efficient since, periodical update and maintenance of such rules are important, which is a tedious process. So, we move for machine learning approach, which uses certain algorithms and requires some sample emails for training and testing purposes, based on which the spam emails are automatically filtered [7], [15].The reason for sending spam contents to users are to trick them for buying a product, or to download a content from websites or to interact with malicious contents which can affect the hardware and software of the user's computers. Another one important reason for internet spamming is to steal the personal online credentials which one refuses to share it with others. Internet marketers are increasing nowadays, so it is important to control malicious and unwanted commercial spam contents which are a major problem in internet. To address this issue and to solve it, coding the contents into a photo and encoding good words without any contexts is practiced. At the end of 2015, there was only 1% of picture spam is identified, but at 2017, about 40% of spams are of picture spams [8].Phishing when associated with hacking is a cybercrime. The term phishing is named after the approach of trapping a fish and snatch it, which is called as fishing. Phishing harms the e-commerce sites by making the users to lose trust on it. To alert the users form phishing attacks, the users are provided with phishing alarms by Anti-phishing Working Group (APWG). In the 1st quarter of 2014, AWPG reports shows that the phishing attacks are increased by 10.7% from the final quarter of 2013. All the messages fall under the following three categories, Ham, Spam and Phishing. The Hams are the legitimate emails, while Spams are the spontaneous emails and the Phishing are the unsafe and spontaneous emails whose target is to imitate the legitimate e-banking emails [9].

In 2006, Twitter, a popular social media site was released which attracted more than 320 million users who actively collaborate with it in daily basis, to share some shot message contents named tweets with 140 characters maximum, and multimedia contents like photos, videos and weblinks. In 2014, Digital Media Rambling (DMR) released a report that show that sharing information in twitter is going on increasing rapidly which attracts the cybercriminals to exploit the trustworthiness of it by sharing malicious contents for many of the twitter users. These cybercriminals are called social spammers who use several techniques to boost their account information. They even use some existing users account information and mimic them as real users. The spammers distribute malicious software like Trojan horse, career-spamming, compromised accounts by using the twitter provided services to achieve their goals [10].Email server is the most used application service for many users in daily basis. Emails acts as a way of communication like sending and receiving text messages and multimedia, then for many users, rely on email accounts for doing their daily tasks on internet, e-banking for providing bills and banking statements, e-commerce websites like Amazon asks for email address from all of their customers to provide their services like promotingthe new arrivals in their shopping site over time and the applications of email are so on. Some spam emails are sent just for entertainment purposes to just waste the time of the users and then for distributing malwares like trojans, viruses etc. and then for advertising, which attracts the users by interesting appearance, texts, images etc. and several other activities for example, giving free rewards, winning contests, etc. to get the attention of the online users[11]. Emails are the fastest, most convenient, easiest and economically cheapest way of communication. But the diffusion of spam emails is the major bottleneck for the usage of emails. Thus, filtering those spam emails are the serious concern for researchers to make email communication more effective. Several approaches in the field of email spamming are developed by the researchers, most commonly with the SVM approach. After that, based on it several other approaches of text classification are also developed. SVM is used in the selection of kernels that partition the emails in quality space results as serious matter [12].

Spam messages are sent through SMS, email and social media. Statistics show that most of the messages in social media are the spam messages. A study from Proofpoint, a company that specializes in the field of cybersecurity reported that at the first half of 2013, the spam messages have attained a growth of 355%. Out of 7 new accounts in online social media, 5 of them are spams. This is due to the fact that the social networks are growing these days and a significant number of communications are done through it. At the second quarter of 2018, twitter has an average of 355 million users actively on monthly basis with lots of genuine contents along with the spam messages, even in the business networks like LinkedIn, which causes a serious threat in both social and economic activities. This issue results in shrinking the growth of productivity and increases the use of technical help desk that causes hindrance in the growth of online networks, also causing threats in losing the privacy in social media networks [13].Since commercialization is growing through internet, spams are also ruling them. Spammers retrieve the personal data of users form various website or viruses and prevents them for using full length bandwidth. The online reviews of customers make great impact among industrialization. The review of customers regarding a product or service helps other customers to purchase it. But if those reviews are in a negative way, it affects the business flow and if those reviews are fake, then it affects the gain of the industries also creates trust issues among the costumers. The spams are distributed in many ways like sending emails in mass in which there will not be any immediate response between the sender and the receiver. So, a spam channel device is used to perceive the spam. But this system cannot be easily formalized and the causes a trust issue, since it does not verify the spam fully [14]. The impact of social networks causes considerable changes in the socio-economic platform and development of organizations. Among them, Facebook, LinkedIn and Twitter are the most leading platforms which use the information provided by the uses for a valuable communication among people. In twitter, all the data are freely available for everyone, so this platform serves as a best platform for the researchers to work on spam detection, event detection, personality identification, sarcasm detection and so on. Twitter has more than 313 million uses active on monthly basis and 350,000 tweets per minutes, which is 500 million tweets per day.Among them, 9.9% of tweets are identified to be spams per week for the sake of private or organizational gain. This spam can be of many categories like sending replies with bold and abusive texts to attract the users, sending hostile links, redundant profile creation and trolls for attention seeking. Often those spam contents have URLs which redirects the users to adult sites or contents that are out of the contexts. This redirection makes the users to enter into mischievous sites that consist of viruses. By spoofing, the personal data of users are stolen and bots are even used nowadays for automatic data stealing from large number of readers per day [16].

The spam emails are causes serious threat in the security of users over internet, since it fills the mailbox with unsolicited emails thereby reducing the storage space and bandwidth also spreads the fake messages and malicious contents easily. Kaspersky lab reported that around 56% of total email traffic consists of spam emails. To address this issues, 2 types of information are taken, viz., content-based and non-content-based information. The content-based information consists of the textual data like email subject, and body. The non-content-based information consists of the email headers, IP addresses, sender addresses, writing style, reputation and sending time. This information is used for detecting the spam emails. The content-based approach is focused by [17] for detecting spams.In past few years, the online social networks act as a platform for getting information, distributing information, entertainment and making friends. The process of tracing the information generation, content creation, effects of user adoption, information distribution, and group interaction are difficult due to the complexity in the structure of online social network. These data create a great impact on the daily life of people in personal and working environment. The spam detection in social networks facilitates analyzes and event monitoring in social media and regulates them [18]. The spam mails are increasing which causes serious threats for years. The spam can be distributed for product sales and also for online fraudulent attacks. Many researchers are working on detecting spams and filtering them, since it is reported that billions of dollars are benefited in underground economy. Kaspersky lab reported that in the second quarter of 2017, 56.97% are spam emails which 2.77% is higher than that of the third quarter of 2015. This shows that the email spams are going on increasing day-by-day, hence due to its criminalization, spams are considered as much dangerous. The spams are getting even more dangerous sue to various issues in social engineering, attachments and language diversity. Spam filtering is important in the field of scientific as well as industries. In [19], the hypothesis of spam detection through personality recognition and sentiment analysis is validated, and expecting to achieve improvements in current techniques of spam filtering.

Emails are one of the cost effective and common communication platforms over internet. Emails can be sent and received by anyone with computer or mobile phones with internet facilities anytime and anywhere in the world. But nowadays, emails are more threatening due to the increase in spam contents. The spams are sent to random users or companies with misleading subject and worse crafted contents that wastes the time of the recipients, money of the marketers and damages the reputation of a company, as well as affects the network usage and capacity by creating several unwanted data. In [20], a machine learning model developed to detect and filter those spam emails that causing much threat is proposed.Spams are not only disturbing the users but also consumes large amount of time and storage space. Around 83% of spams are dangerous, since the URLs in it redirects to some phishing websites which causes Trojan attacks within a click that infects the computers with viruses or make the deceiving some malicious links. Also, it occupies additional bandwidth and causes delay in messaging service. These problems can be solved only by the effort of administrators manually. At that time, there may be a possibility of some important emails to get deleted while deleting a huge number of spam emails [21].Based on the reports from McAfee Lab, in the fourth quarter of 2016, the KelihosBotnet exist in the first position which is 95% of the volume in third quarter. Kehilos is most common in spamming pharmaceuticals, then it targets the Chinese have job offers in which Botnet of type lethic size of 60% over the fourth quarter, basically who pushes the knock-off designer wrist watches. If this spam gets continued in the same level, then the overall spam cost in business will reach $257 billion per year. The recent report released in March 2011 says that over 83.1% of spam emails are from Botnets. These botnets are of less cost and deployed easily, but hard to detect, so that it compensates financially the Botmasters [22].

The opposite of spam is the ham. The term "spam" is derived from "Shoulder Pork HAM", which is a canned precooked meat sold in 1937 and named the same for the digital mailing junk which exists at the same time. The spam emails are helpful for the marketers for unfolding malicious practices like reputational damage and financial disruptions in both organizational and personal activities. In course of the spams are spreading in the platforms other than email also. The major target of the spammers is the financial motivation, which makes them getting around $3.5 million every year from the spams [23]. Due to the vast development of internet, email is an essential way of communication among the society due to its fast delivery, minimum cost and reliability. The use of emails increases worldwide, eventually the spam emails are also gets increasing. A statistical report in 2009 says that over 1.4 billion emails are sent in a day which is doubled in 2013. Over 70% of business emails are spam emails. These spam emails cause critical problems like reducing the bandwidth of communication, wasting the storage space by filling the mailbox, and wasting time of the users by making them delete all those spam messages, also damages the computers by viruses etc. The spam emails usually vary in contents, but most of them are commercial adverts. Many researchers and companies are involved in developing anti-spam software, but none of them are expected to get 100% results, since the spams are varied according to the current trend and knowledge. The traditional way of filtering spams no longer supports in recent technologies [24]. A semi-supervised approach of machine learning method of email classification is employed in [25]. The supervised approach of machine learning requires high cost for collecting labeled data, since the labelling should be manually given by specified analysts. But the unsupervised data doesn't need any labelled data, which can be easily collected. So, a semi supervised approach which combines a little of labeled data and a large amount of unlabeled data are collected and used as the dataset for spam email filtering software. The semi supervised approach involves in labeling all the unlabeled data with the help of labeled data to maximize the dataset size thereby increasing the accuracy of the software [25].

The objective of the study is given as follows:

- Reviewing the susceptibilities of spam emails and the threats caused by it.
- Explaining about the research methodology conducted in this study.
- Survey on various existing techniques involved in the process of filtering spam emails.
- For the better understanding of spam emails and its consequences, the basic knowledge about spams are discussed.
- Providing a detailed descriptionof proposed algorithm for the detection of spam emails.
- Finally conducting performance evaluation and concluding the overall contribution of the study followed byproviding future suggestions.

II. Research Methodology

Identifying the problem statement is the first step in conducting a research. Detecting the spam emails are a complex and challenging task. Creating a model for the classification of spam and legitimate messages is difficult yet important, inorder to protect the users from phishing emails for identity theft and from accessing the online account details. The flow diagram of research methodology is illustrated in Fig.1.

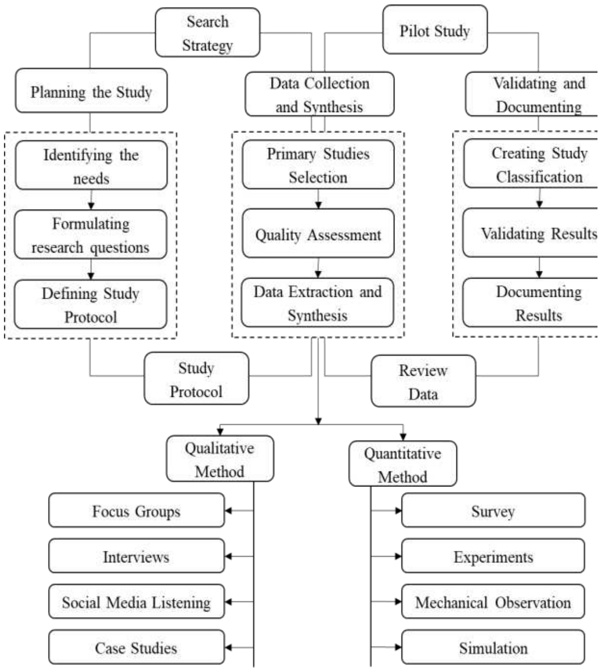

Fig.1Flow Diagram of Research Methodology

After the identifying the need for the study, some research questions are formulated so as to compare the efficiency, feasibility and performance of existing methods and user requirements in the field of spam email detection and then to define the study protocol. This can be done by selecting some primary research studies. The data from the selected studies undergo a quality assessment. The data from the screened studies are extracted and synthesized based on the requirements. The primary data extraction methods are Qualitative and Quantitative methods. The Qualitative data are extracted based on the focus groups, interviews, social media listening and case studies. The Quantitative data are extracted based on the surveys, experiments, mechanical observations and simulation. Another one type of data extraction is the mixed method, which is the combination of both qualitative data and the quantitative data.

Finally, the classification parameters are created and the results are validated for accuracy and loss percentage. These results are then documented and reported.

III. Related Work

In [1], the phishing emails are classified based on machine learning approach. For this, "The Short Message Service Spam Collection v.1" dataset is used. This dataset contains 5574 tagged spam and ham real, non-encoded messages in English language. Algorithm such as Natural Language Processing, NLTK and Scikit-learnare used for text classification and analysis of phishing datasets. Classifiers such as Decision Tree, SVC, Random Forest and K-Nearest Neighbor are used for spam and ham classification. This method is implemented in python using Anaconda Jupyter lab [1]. The spam mails are traditionally classified using supervised classification model. But it is found that, the supervised approach of spam detection is hard to maintain. Thus, [2] investigated a hypothesis that, this system is reliable for spam detection even the recall will be far from perfect. This hypothesis is implemented by using the outcome of previous supervised spam detection system as a graphical model framework which is considered as a tool for detecting spammers. The proposed approach is built using a Markov Random Field on similar user graphs,and figure out prior beliefs by selecting state-of-the-art classifiers. The posterior prediction is obtained by using Loopy Belief Propagation. This model is examined using a recent Twitter dataset which was collected by the researcher and labeled manually. The results show that there is a significant improvement in recall and a maintained precision. Thus, it is determined that, by using undirected graphical model framework helps in restoring the performance of existing statistical classifier for detection problem and to successfully mitigate the impact of evolution of spams [2].Even though various spam detection methodologies exist, the results obtained by them are not much satisfying. Many of the malicious sites still escape form the spam detection techniques. Thus in [3] three types of spam detection techniques are summarized at first, namely Hidden Iframe, Redirection Spam and Content Hiding Spam. Thus, a new spam detection method is adopted that captures the screenshot of malicious websites to invalidate web spams. This proposed method is built by Convolutional Neural Network (CNN) for classification and the classification outcome is verified using 2 experiments. One is by using a complex dataset and comparing the results of proposed approach and other algorithms. The second is by detecting the malicious websites in real time internet sites for 3 months and found that the proposed approach gives a better performance practically [3].

Creating fake accounts that look like a genuine account are much easy nowadays and do fraudulent activities like sending malicious links through spam emails that harm the computers of users. That target people of the spammers are those who are unaware of the spam contents. Thus, machine learning algorithms like Naïve Bayes, Support Vector Machine, K-Nearest neighbor and ensemble learning approaches like Random Forest Classifier and Bagging areapplied on the datasets which are used to detect spam emails and the algorithm that produces best result of spam detection with higher precision and accuracy is identified and selected for spam email detection [4].In [5], the IOT cyberspace is taken into account for detecting spams in IOT based social media applications. It is divided into 2 patterns, namely Behavior pattern and Semantic pattern-based approaches. Both patterns are collaborated and developed a new method that relies on multi-source information fusion, called Collaborative neural network-based spammer detection mechanism in social media applications. This method is examined using experiments conducted on 2 real world datasets with different parameters. The results from the proposed approach is compared with 5 baseline approaches based on some evaluation metrics and found that the performance is improved around 5% when compared with the baselines [5]. Due to the influence of e-reputation on the success of several organizations, spammer provides fake reviews that affect the reputation of a company's service or products. Thus, a novel method based on Evidential K-Nearest Neighbor (EKNN) algorithm is proposed in [6] to detect those spam reviews, by using the theory of belief function. This method depends on the spammers indicators as features to classify the genuine and spam reviews. The efficiency of this system is tested with a real world labeled dataset from yelp.com [6].

In [7], Logistic Regression, a most popular algorithm is used for classification of spam emails, and Natural Language Processing for reading, deciphering and understanding the human languages and the outcomes are compared with the results obtained by K-Nearest Neighbor classifier.Images are a major part of communication among people, but nowadays images hide or embed some spam messages, which contains harmful contents and those spam images are circulated in social media and in emails. Thus in [8], a spam detection model which uses Optical Character Recognition for extracting texts from images, combined with Natural Language Processing for extracting the natural human languages for detecting and classifying the usual texts and human slang contents. Bag-of-words model is used for feature extraction from those images with the machine learning algorithm to execute the spam classification model [8].To detect the phishing attacks in email networks, a novel hybrid approach which combines the Natural Language Processing, Support Vector Machine and Probabilistic Neural Network is used for feature extraction and classification. The features are extracted using NLP from the datasets and the extracted features are used for classification using combine SVM and PNN based classifier for classifying phishing emails [9].

Twitter is a major platform for several social activities like microblogging and for news updates. This makes the cybercriminals get attracted to twitter for cyberattacks. The spammers make use of Twitter to spread malicious links, spam messages and flood them with fake profiles for malicious activities. Thus, it is important to detect the network of spammers who spread spam messages to identify individual spam accounts. Although several researchers proposed various techniques for detecting spammer groups, they all focus on only some of the groups. Hence, in [10], a new approach is introduced, that detects various spammer groups based on the similarities of the contents provided in the spam accounts. To improve the performance of the classifiers, many features are extracted. The proposed system uses principal component analysis and tuned K-means clustering on 200,000 accounts and selected 2 million tweets randomly to detect the spammers cluster and attained the result of 96.3% of accuracy for Random Forest classifier, which is the highest, then 95.6% accuracy for SVM and 96% for multilayer perceptron approach. Also, the Random Forest classifier achieved the highest precision, accuracy, recall and F-measure [10].Classification of spam and non-spam emails is a challenging yet important one, due to the wide spread of spams and phishing contents on internet sites. The Artificial Neural Network (ANN) based data mining in the detection of spam messages are more prone to errors in detection result. This is because the training data consists of most of the spam features. So this error can be reduced by using Sine-Cosine Algorithm (SCA) based feature selection and the selected feature vectors helps in selecting optimal features for training purpose. The proposed method of Spambase dataset in MATLAB results in 98.64% precision, 97.92% accuracy ad 98.36% sensitivity, which shows that the proposed system outperformed the Multilayer Perceptron Neural Network, Decision Tree, Bayesian Network and Random Forest classifiers in detection of spams. Also, the results show that the Multilayer Perceptron NN based feature selection error is decreased by 2.18% [11].The dataset is split into two with a large part for training the classifier and a small part for testing the classifier. The features are extracted only if the threshold value is 70% and 50%, else it is discarded. Relief method is employed for calculating proxy statistics of the features from the dataset, which is then used to calculate the rank of the feature. The attribute value can be calculated by multiplying the threshold value with the number of attributes. If the rank is greater than or equal to the attribute value, then the relevant feature is extracted otherwise, the feature gets discarded. To get the membership degree, Fuzzy C-means clustering algorithm is used and SVM with polynomial kernel function is used for classification, which is simply called as FSVM approach, which is well suited for datapoints with unmodeled characteristics [12].

The machine learning techniques like neural networks, SVM and Naïve Bayes classifiers are not much efficient and require complex features. These techniques cannot reduce the errors with cost variations. Thus in [13], a cost-effective novel method of spam filtering method is proposed which consists of 2 stages. The first stage is a multi-objective evolutionary feature selection is followed for reducing the cost of mis-classification and the number of attributes required to filter the spams. The second stage uses a cost sensitive ensemble learning approach with regularized deep neural network ad base learners. This proposed model is implemented with 2 benchmark datasets and the results produced outperform various other algorithms like SVM, Naïve Bayes and Random Forest algorithms [13].A Long Sort Term Memory (LSTM) layers in Recurrent Neural Network (RNN) approach is used for detecting electronic junk emails which is also known as spam emails. This method simplifies the representation of texts into words which can lead to getting higher rate of accuracy. RNN with embedded and LSTM layers is used for sequence-to-sequence task is used in [14]. The neural network takes a series of raw texts as input and gives a sequence of labeled predictions as output. The model is built with 150 neurons in input layer and then the LSTM layer followed by a dense layer genuine enactment work and then a drop-out layer, then another one dense layer which is then followed by another dense layer at last with sigmoid actuation work in sequential order. The last layer has 2 output classes for spam and hamemails [14]. In [15], the performance of various email spam detection techniques based on different types of algorithms are evaluated and with the final outcome, an effective model for spam email detection through machine learning algorithm is suggested. For this experiment, UCI Machine Learning Repository Spambase Dataset is used, which is applied on machine learning algorithms like, KNN, Naïve Bayes, Logistic Regression, SVM and Decision Tree for performance evaluation. For training and testing purposes, Weka tool is employed [15].

To overcome the problem of spam distribution in Twitter, [16] proposes an approach that focusses on both the profile and content-based detection of spams. a technique called NLP is used to create new comprehensive dataset which consists of several content-based features, then this dataset is given to a hybrid machine learning model. At last, logistic regression is used to differentiate genuine users and spammers [16].The use of text semantic analysis is explored for better spam detection, in which there are 2 semantic levels. The first level is, the emails are categorized based on Education, Health, Financial domains etc. Then the second level combines the manually specified and automatically extracted semantic features in each of the domains. The extracted features are used to differentiate the spam emails from non-spam emails effectively. The results of this approach show that it provides better accuracy in spam detection when comparing with Bag-of-Wordsand semantic contents [17].The unbalanced data distribution caused by spam and non-spam messages in Twitter is solved by analyzing spam characteristics from Twitter by using Improved Incremental Fuzzy kernel regularized Extreme Learning Machine (I2FELM) for accurately detecting Twitter spam. This I2FELM detects the balanced and unbalanced dataset efficiently with few characteristics, thus proves its effectiveness in spam detection [18].

There are several techniques available for detecting spam emails. But the hypothesis that the spam emails can be identified by sentiment analysis and personality recognition approaches are evaluated. The new features provided by these techniques helps in improving existing spam classification approach. Thus, in [19], the sentiment analysis and spam classification techniques are combined to analyze the email messages. The extracted new features are added to existing dataset individually and then combined to compare the results of several best spam email filters and classifiers [19]. Various machine learning algorithms like Naïve Bayes, Random Forest, and SVM are used for spam email detection and their accuracy is evaluated. The result shows that Random Forest classifier has an accuracy of 0.97 which is better than that of Naïve Bayes with accuracy 0.93 and SVM of accuracy 0.90 [20].The problems such as limited capacity of mailbox, security of personal email and loss of bandwidth for communication arouse form botnets available world wide in internet field for spreading spam emails are addressed by using an Online Botnet Spam Email Filtering Framework (BSEFF) which makes use of Neucube algorithm, a new Spiking Neural Network (SNN) architecture and Adaptive Dynamic Evolving Spiking Neural Network (deSNN) algorithm is proposed. This algorithm handles larger and faster spatio-temporal data by using SNN as core processing technique. It is believed that this method is the first in using Neucube algorithm for spam detection and the BSEFF inherits the features of this algorithm that adopts both supervised and unsupervised machine learning in an online framework with long life learning for classification of inputs while the framework is learned [21].

The most important yet challenging process in data mining is the Feature Selection in pattern recognition. In [22], a new hybrid model of Whale Optimization Algorithm (WOA) and Flower Pollination Algorithm (FPA) is proposed for the issues caused in feature selection based on Opposition-based Learning (OBL) named as HWOAFPA. At first, WOA is executed, at the same time population of WOA is varied by OBL. It is employed as the initial population of FPA to improve the speed of convergence and accuracy. The performance evaluation of the proposed approach is done in 2 steps namely, experiments on 10 datasets from UCI Data Repository and on Email Spam Detection dataset. The experiment on UCI Data Repository dataset provides more successful average size of selection and classification accuracy in comparison with basic metaheuristic algorithms. The results form Email Spam Detection dataset provides more accurate detection of email spam when compared with other similar algorithms [22]. In [23], a survey on various intelligent email spam detection techniques based on Artificial Intelligence and Machine Learning approaches are employed. For this, four parts in the structure of email are considered for analysis. They are Headers Provide Routing Information like Mail Transfer Agents, SMTP Envelope which contains identification and domains of users, First part of SMTP Data like from, to, data and subjects, and Second part of SMTP Data like body text and attachments.According to the number of relevance of a method, the research paper is identified, read and summarized in this survey and the findings and challenges are briefly explained which provides suggestions for future researches on theoretical and empirical aspects in the field of email spam detection [23].Although, SVM is widely used in the detection of spam emails, it experiences a serious issue when dealt with huge data, like time and memory consumption and less accuracy. To overcome these issues, a hybrid approach of SVM and K-means clustering technique with number of clusters, which is named as K-means SVM (KSVM) algorithm is used. The computational speed of SVM can be increased by minimizing the number of support vectors. This approach is experimented using the Spambase standard dataset for evaluating its feasibility and also reduces the computational time, speeds-up the emails transmission and improves the accuracy. The result shows that the proposed KSVM approach outperforms in classification accuracy and efficiency [24]. Due to the development in emails for communication and content sharing, since it is the cheapest and fastest platform for communication nowadays either personal or professional, a large part total internet traffic isfrom emails. Hence, it is important to automatically analyze the contents of the email, since emails are also the source of spreading spams and has security issues and deceptiveness due to spammers nowadays. Therefore, an iterative standard EM-based semi-supervise learning approach is introduced for automatically detecting spam emails. This approach involves 2 steps. At first, the labels of unlabeled samples are predicted and labeled using the current classifier such as the Naïve Bayesian and K-nearest neighbor classifiers, built in the previous iteration.Second, a new classifier is reconstructed with the labeled set of new training samples. This system reduces the execution time, and increases the classification accuracy [25].

IV. PROPOSED NATURAL LANGUAGE PROCESSING BASED RANDOM FOREST METHODLOLGY

The reason behind spam emails are the tricking the recipients by sending fake emails and making them believe that it is from legitimate source for identity theft or stealing login credentials of accounts etc. These fake emails can be created by breaking the web server with relevant phishing tools. This email is then sent with a malicious link or malicious content to the recipient. This malicious content is opened by the recipient, which redirects them to malicious website or asking for their personal details or online account credentials which is then misused by the attacker. The techniques used for creating this type of fake emails are social engineering, malicious cods, wireless medium, subterfuge, screen capture and key loggers. Email phishing is the most common method of phishing attacks, since most of the important and official communications are done in emails. Thus, it is easy to steal the personal data of a recipient through the spam emails.

Email addresses are the most important source of personally identifiable information in internet. Most of the websites available, asks for email address for their registration and further usage including password recovery purposes. But the email addresses are not protected. When registering on an online social website, malicious third party can easily access the email address of a person which exposes them to spam and phishing attacks. Sometimes the email address can also be leaked with passwords which can be used for linking several web services with it. To overcome this serious issue of registering into some of the networks like online dating services, a temporary email address can be created and used, which are disposed after a short period of time by the service providers, so that any spam and phishing attacks can be subjected for that temporary email account and does not reveal any real identity. But the temporary email accounts are also used by spammers, which causes serious security threat to distribute spam messages and trojans via malicious contents. This could also be analyzed seriously and should take necessary measures to detect those temporary email addresses and prevent identity theft and security threat.

A. *Spam Emails*

The aim of sending spam emails are the entertainment, malware spread, advertisement, information theft, etc. These spam emails are sent to the users without their permission by the spammers and it targets to attract and seek the attention of users. The spam emails include a particular pattern to be repeated like the texts and images related to money, career and payment activities. It deceives the uses and leads them into phishing attacks. The false URLs sent to a user via email seem to be a legal one, so that it is a great challenge to identify it. Also, several other spams contents can be found on social media, emails and in user comments. Thus, it is found that sending and receiving spam contents are not only through emails, but they are spreading in all over the internet. These malicious links when accidentally clicked, redirects the users to an unsolicited website, that might deceive the users or steals their personal information or leads to phishing attacks or transmits trojans even asks for user online credentials, and once it is submitted unknowingly by the users, then those account details are stolen easily by the attackers. Table I shows the impact of spam emails and its relation with online theft in various services. Most of the spam emails are found to be sent by financial websites that aims in stealing the real identity of the users. It is found from the table, that about 26.10% of spam emails are from email services and about 20.40% of spam emails are form financial services.Fig.2 shows the graphical representation of the spam emails and its relationship with online theft.

TABLE I. SPAM EMAILS WITH ONLINE THEFTS

S.No	Services	Spam %
1	Email services	26.10%
2	Financial services	20.40%
3	Payment services	16.10%
4	Cloud storage	13.80%
5	E-Commerce	7.60%
6	Software services	7.10%
7	Social networks	4.50%
8	Others	4.40%

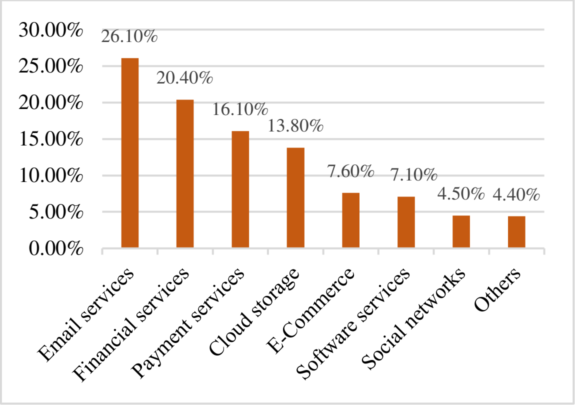

Fig.2 Spam emails with online thefts

Table II represents the phishing attacks via compromised accounts, malware infections and loss of datahappened over three years i.e., from 2016-2018. The data shows that the phishing due to compromised accounts are more common and also shows that the phishing attacks goes on increasing and never falls down.Fig.3 shows the graphical representation of phishing attacks over the year ranging from 2016-2018.

TABLE II. PHISHING ATTACKS OVER 2016-2018

S.No	Way of Threats	Year	Phishing %
1	Compromised accounts	2018	65%
2		2017	38%
3		2016	17%
4	Malware Infections	2018	49%
5		2017	49%
6		2016	27%
7	Data Loss	2018	24%
8		2017	13%
9		2016	7%

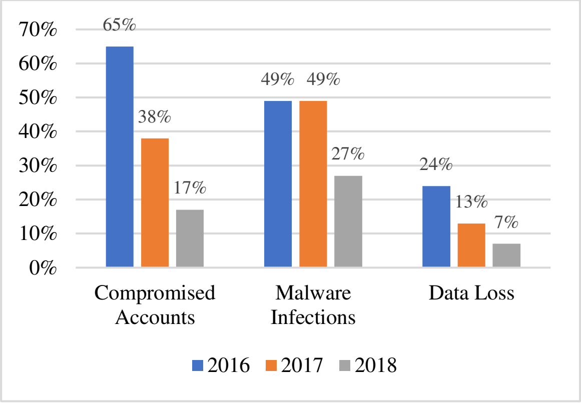

Fig.3 Spam emails with online thefts

There have been a number of researches in detecting, classifying and preventing spam emails. In this study, the Natural Language Processing (NLP) and Random Forest Classifier are used for detecting and classifying the spam emails. Text classification and analysis of spam dataset is carried out by NLP. Random Forest Classifier is used to classify the emails into spam and legitimate emails.

The NLP helps computers to communicate with humans. NLP can hear, read, edit and interpret texts, speech and identify the import parts in it. NLP removes stop-words, punctuations, stemming, tokenization, tagging, identifying semantic relationship and language detection automatically with the help of software. The Random Forest Classifier is formed by various kinds of decision trees which are of multiple size and shape. The randomness of this classifier reduces generalized errors by less correlation. The block diagram of the proposed NLP-RF method is shown in Fig.4.

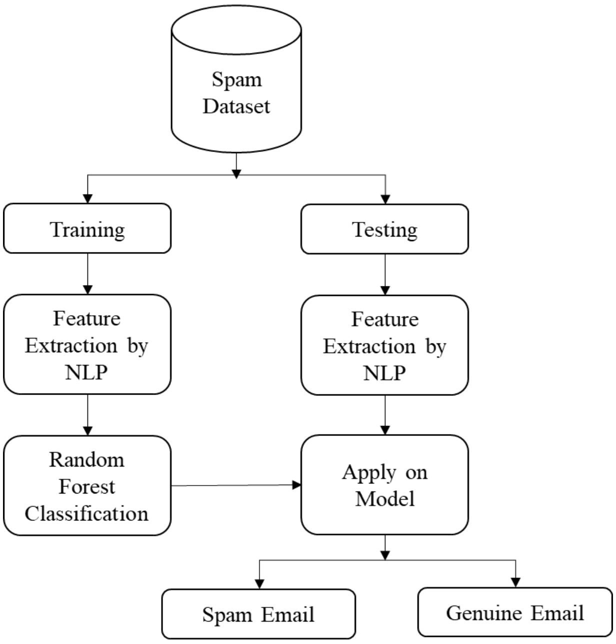
Spam Dataset
Training
Testing
Feature Extraction by NLP
Feature Extraction by NLP
Random Forest Classification
Apply on Model
Spam Email
Genuine Email

Fig. 4.Block Diagram of Proposed System

The first step in our proposed system is to import necessary libraries needed for execution of algorithm. Then the created spam dataset is loaded. Before creating a model, the data must be pre-processed. This can be done with the help of Natural Language Processing (NLP) algorithm by converting the whole text data in to lower-case letters, removing the numbers, punctuations and stop words, stemming and tokenization. After pre-processing, the next significant phase is the feature extraction. Feature engineering helps in generating the relevant features in the data using domain knowledge which is used by the machine learning algorithm. The features are in the form of tokens and the unimportant features generated are removed for better classification. After creating a dataset, it is then split in a ratio into train dataset and test dataset. The train dataset is used to build a model and to train the classifier whereas the test dataset is used to validate the model which is built for classification. The classifier used for detecting the spam email in this approach is the Random Forest Classifier. Finally, the accuracy rate is calculated and then the system is improved for better classification.

B. Natural Language Processing

Natural Language Processing (NLP) is a branch of Artificial Intelligence (AI) which involves communication among humans and computers with natural languages. The main aim of NLP is to read, decipher, and understand and to make sense of languages followed by human beings in a valuable manner. Most of the techniques involved in NLP depend on Machine Learning (ML) to find out the meaning of human languages which can be employed as follows:

- Humans interact with computing systems.
- Audio captured by devices.
- Conversion of audio to text.
- Text data processing.
- Data to audio conversion.
- Device plays the audio as the outcome.

NLP includes using algorithms for identifying the natural language rules and extract them, like converting an unstructured data into computer understandable forms. The texts entered into a computer makes use of certain algorithms to extract the connotation of those texts with every sentence and gets the required data from it. There might be possibility of not understanding certain text data, which leads to obscured results. The below are the syntax techniques involved in NLP process.

1) *Lemmatization*: It involves reducing several modified forms of a word in to one form.

2) *Morphological segmentation*: This technique divides the words into individual units called morphemes.

3) *Word segmentation*: This technique divides larger pieces of a continuous text into distinct units.

4) *Part of speech tagging*: This technique identifies the parts of speech for each word.

5) *Parsing*: This technique analyses the grammar in the given sentences.

6) *Sentence breaking*: This technique places boundaries for sentences on large text.

7) *Stemming*: This technique cuts the modulated words to its root form.

The below algorithm (Algorithm 1) gives the pseudocode for Natural Language Processing approach.

Algorithm 1: *Natural Language Processing*

```
Start
for each d in document:
  pCount = Σ (no. of paragraphs)
  Tokenize d by paragraph
  FakeRank = 0
end for
for each paragraph in d:
  qScore = Σ (no. of paragraphs)
  if qscore> 0
    for each quoteset
      quote_c1 classify.randomforest
      (quoteset_attribution_space, d)
      if quote_c1
        A-score = A-score+1
      else
        A-score = A-score-1
        return A-score
      end if
    end for
    FakeRank = FakeRank + A-score
  ifFakeRank>= 0, then
    dLabel = real
  else if FakeRank< 0, then
    dLablel = fake
  end if
end for
end
```

C. Random Forest Approach

The Random Forest (RF) approach is most commonly used for feature selection and classification purposes in data science. This is due to the fact the node purity is improved by a tree-based approach of RF algorithm. Nodes with fewer impurities will be on the starting part of the trees and nodes with more impurities will be on the ending part of the trees.The decrease in mean impurity allover the trees is called Gini impurity. Thus, by trimming the trees below a particular node, a best subset is generated which provides highly accurate results. The RF approach consists of 4 to 12 hundred decision trees in which each node is built randomly. The decrease in impurity is averaged across the trees for final prediction. Algorithm 2 shows the steps involved in Random Forest approach.

Algorithm 2: *Random Forest Approach*

```
Start
Generatingn classifiers:
for $i = 1$ to $n$do
    Training sample $S$ randomly selected and replacedby $S_i$
    Creating root node, $N_i$with$S_i$
    Call BuildTree$(N_i)$
end for
BuildTree$(N)$:
if $N$having single classthen
    return
else
    $x$% of splitting features in $N$is selected randomly
    Selecting feature,$F$ with more information for splitting
    Creating$f$ child nodes of $N, N_1, \dots, N_f$,
        where, $F$ contains $f$ possible values $(F_1, \dots, F_f)$
    for $i = 1$ to $f$do
        Set contents of $N_i$ to $S_i$,
            where, $Si$ = all of the matching instances in $N$
$F_i$
            Call BuildTree$(N_i)$
    end for
end if
end
```

D. Machine Learning In E-Mail Classification

Machine learning is a part of AI, which helps machines to learn like humans. In this technique, the machine observes, understands and represents the information fed to them. The email spam filtering can be carried out by using the dataset containing certain set of texts and subject lines. The process involved in filtering spam emails are (1) Data collection and representation which is of problem-specific, (2) Feature selection which is used for further processes and finally (3) Spam classification which discovers the actual mapping among training and testing datasets.

1) Email pre-processing: The information from the email contents are extracted and stored in a database. They are then converted into feature vectors with several attributes. The attribute was set if the relevant word exists in the text message and 0 else.

2) Feature Extraction: In this step, the features are extracted. The features include spam and ham texts which are stored in the form of dictionary and feature vectors which are provided as an input to the algorithms. The feature extraction is used for training and testing the classifier. The extracted features are converted into feature vectors for further processes.

3) Spam Classification: From the above steps, the training documents are found and are pre-processed for extracting useful information and stored as texts, which are then split into words. Then the features are extracted and converted into vectors of fixed format. Finally, an optimal classifier is employed for classification of spam and ham emails and filter them.

4) Performance Evaluation: The performance of the proposed approach is evaluated finally to calculate the accuracy of the proposed algorithm and if needed, the approach can be improved to attain better results.

The below alorithm (Algorithm 3) gives the overall process steps for spam and ham email classification using Random forest classifer.

Algorithm 3: *Overall steps for spam email classification*

```
Start
Input$X$ = Number of nodes
Input$N$ = Number of features in Email Message
Input$Y$ = Number of trees
while termination condition ! True do
    Selecting self-staring Email Message $S$extensively from
training corpus $Y$
    Creating tree $R$?? from selected self-starting Email
Message,$S$
    Choosingn features arbitrarily from $N$; where $n << N$
    Computing optimal dividing point for node $d$ among $n$
features
    Dividing parent node to 2 offspring nodes through
optimal divide
    Execute till maximum number of nodes $(x)$got created
    Creating forest for $Y$ number of times
end while
    Generating resultsfor every tree$\{R_t\}_1^Y$
    Using new Email Message for every tree starting at root
node
    Designate Email Message to groups that are compatible
with the leaf node.
    Merge results of every tree
return Final Email Message Classification group having
the highest vote $(G)$.
end.
```

V. Performance Evaluation

The Classification Accuracy(A_{cc}), a spontaneous approachis defined as the ratio of sum of predicted numbers (True Positives and True Negatives) and corrected predicted numbers (True Positives, True Negatives, False Positives and False Negatives). It can be mathematically expressed as,

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} * 100$$

Where,

TP = True Positive, it is the rate at which the ham emails are detected efficiently.

TN = True Negative, it is the rate at which spam emails are detected efficiently.

FP = False Positive, it is the rate at which spam emails are detected wrongly and

FN = False Negative, it is the rate at which spam emails are detected wrongly.

The Precision is defined as the ratio of True Positives to sum of True Positives and False Positives. It is also referred to as Positive Predictive Value (PPV) and can mathematically be expressed as,

$$Precision = \frac{TP}{TP + FP}$$

The Recall is defined as the ratio of True Positives to sum of True Positives and False Negatives. It is also referred to as Sensitivity or True Positive Rate and is mathematically be expressed as,

$$Recall = \frac{TP}{TP + FN}$$

The F-Measure (F_{m})is defined as the weighted average of Precision and Recall. It is better than the classification accuracy, if in case the class distribution is not even. If the cost of FP and FN are not the same, then F-Measure is more suitable for performance calculation. The F-Measure mathematically can be expressed as,

$$F_m = 2 * \frac{Precision * Recall}{Precision + Recall}$$

True Negative Rate (TNR) is defined as the ratio of True Negatives to the sum of True Negatives and False Positives, which can be expressed mathematically as,

$$TNR = \frac{TN}{TN + FP}$$

False Negative Rate (FNR) is defined as the ratio of False Negatives to the sum of False Negatives and True Positives, which can be expressed mathematically as,

$$FNR = \frac{FN}{FN + TP}$$

False Positive Rate (FPR) is defined as the ratio of False Positives to the sum of False Positives and True Negatives, which can be expressed mathematically as,

$$FPR = \frac{FP}{FP + TN}$$

VI. ACKNOWLEDGMENT

The authors extend their appreciation to the Deanship of Scientific Research at Jouf University for funding this work through research grant No (DSR2020-06-3680)

VII. CONCUSION AND FUTURE SCOPE

Spam emails are one of the critical issues over internet in recent communication systems. Spammers send spam emails by misusing the facilities in the online communication by various methods, including sending spam emails by using temporary email addresses that affects the users and involved organizations. In this paper, a method of Natural Language Processing based on Random Forest approach (NLP-RF) is proposed which helps in easily detecting spam emails and temporary email addresses effectively that violates the privacy of users and prevents exposing private data of the users. This method can enhance the privacy of email sender and recipients and reduces security risks and in future the work is subjected to get better progress and accuracy by boosting the dataset for better features and classification systems.

Ethical Compliance

Not applicable

Conflicts of Interest

There is no conflict of interest

Funding

There is no funding

Authorship contributions

All authors have seen the manuscript and approved to submit it to the journal

Acknowledgments

All authors have seen the manuscript and approved to submit it to the journal.

REFERENCES

[1] Priyanka Verma, Anjali Goyal and Yogita Gigras, “Email phishing: Text classification using natural language processing.”, Computer Science and Information Technologies, Vol. 1, No. 1, May 2020, pp. 1~12, ISSN: 2722-3221, DOI: 10.11591/csit.v1i1.p1-12.

[2] Nour El-Mawass, Paul Honeinea, Laurent Vercouterb,“SimilCatch: Enhanced social spammers detection on Twitter using Markov Random Fields.”, Information Processing and Management 57 (2020) 102317.

[3] Dongjie Liu and Jong-Hyouk Lee, “CNN based Malicious Website Detection by Invalidating Multiple Web Spams.”,Information Technology Research Center, 10.1109/ACCESS.2020.2995157, IEEE Access.

[4] Nikhil Kumar, Sanket Sonowal, Nishant, “Email Spam Detection Using Machine Learning Algorithms.”, Proceedings of the Second International Conference on Inventive Research in Computing Applications (ICIRCA-2020), IEEE Xplore Part Number: CFP20N67-ART; ISBN: 978-1-7281-5374-2.

[5] Zhiwei Guo, Yu Shen, Ali Kashif Bashir, Muhammad Imran,Neeraj Kumar, Di Zhang,Keping Yu, “Robust Spammer Detection Using Collaborative Neural Network in Internet of Thing Applications.”, University of Glasgow, 10.1109/JIOT.2020.3003802, IEEE Internet ofThings Journal.

[6] Malika Ben Khalifa, Zied Elouedi, Eric Lefevre,“An Evidential Spammer Detection based on the Suspicious Behaviors’ Indicators.”, Auckland University of Technology. August 11,2020.

[7] Rajavardhan Reddy Marikanti, Katkoori Shiva Prasad, Hannoop Kumar Suddala, K. Bala Thripura Sundari, “Detection of Phishing Attacks using Natural Language Processing and Logistic Regression Model.”, UGC Care Group I Listed Journal, ISSN: 2278-4632, Vol-10 Issue-6 No. 1 June 2020.

[8] Yaseen Khather Yaseen, Alaa Khudhair Abbas, Ahmed M. Sana,“Image Spam Detection Using Machine Learning And Natural Language Processing.”, Journal of Southwest Jiaotong University,Vol. 55 No. 1 Feb. 2020,ISSN: 0258-2724 DOI：10.35741/issn.0258-2724.55.2.41.

[9] Abhishek Kumar, Jyotir Moy Chatterjee, Vicente García Díaz, “A novel hybrid approach of SVM combined with NLP and probabilistic neural network for email phishing.”, International Journal of Electrical and Computer Engineering (IJECE), Vol. 10, No. 1, February 2020, pp. 486~493, ISSN: 2088-8708, DOI: 10.11591/ijece.v10i1.pp486-493.

[10] Kayode Sakariyah Adewole, Tao Han, Wanqing Wu, Houbing Song, Arun Kumar Sangaiah, “Twitter spam account detection based on

clustering and classification methods.", The Journal of Supercomputing, https://doi.org/10.1007/s11227-018-2641-x.

[11] Rozita Talaei Pashiri, Yaser Rostami, Mohsen Mahrami, "Spam detection through feature selection using artificial neural network and sine–cosine algorithm.", Mathematical Sciences https://doi.org/10.1007/s40096-020-00327-8.

[12] Lovely Bansal, Dr. Nirupama Tiwari, "Feature Selection based Classification of Spams Using Fuzzy Support Vector Machine.", Proceedings of the International Conference on Smart Electronics and Communication (ICOSEC 2020), IEEE Xplore Part Number: CFP20V90-ART; ISBN: 978-1-7281-5461-9.

[13] Aliaksandr Barushka, Petr Hajek, "Spam detection on social networks using cost-sensitive feature selection and ensemble-based regularized deep neural networks.", Neural Computing and Applications https://doi.org/10.1007/s00521-019-04331-5(0123456789().,-volV)(0123456789,-().volV).

[14] D Ganesh Kumar, M Kameswara Rao, K Premnath, "A Recurrent Neural Network Model for Spam Message Detection.", Proceedings of the Fifth International Conference on Communication and Electronics Systems (ICCES 2020), IEEE Conference Record # 48766; IEEE Xplore ISBN: 978-1-7281-5371-1.

[15] Nandhini.S, Dr.Jeen Marseline.K.S, "Performance Evaluation of Machine Learning Algorithms for Email Spam Detection.", 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), 978-1-7281-4142-8/20/$31.00 ©2020 IEEE 10.1109/ic-ETITE47903.2020.312.

[16] Ratul Chowdhury, Kumar Gourav Das, Banani Saha, and Samir Kumar Bandyopadhyay, "A Method Based on NLP for Twitter Spam detection.", 26 July 2020, doi:10.20944/preprints202007.0648.v1.

[17] Nadjate Saidani, Kamel Adi , Mohand Saïd Allili, "A semantic-based classification approach for an enhanced spam detection.", Computers & Security 94 (2020) 101716.

[18] Zhijie Zhang, Rui Hou, And Jin Yang, "Detection of Social Network Spam Based on Improved Extreme Learning Machine.", Digital Object Identifier 10.1109/ACCESS.2020.3002940.

[19] Ezpeleta, Enaitz, et al. "Novel email spam detection method using sentiment analysis and personality recognition." Logic Journal of the IGPL 28.1 (2020): 83-94.

[20] Ghosh, Sudipta, and Subhojit Jalal. "Email Spam and Malware Detection Using Machine Learning.", International Research Journal of Modernization in Engineering Technology and Science, Volume:02/Issue:09/September -2020, Impact Factor- 5.354, e-ISSN: 2582-5208.

[21] Alauthman, Mohammad, and Omar Almomani. "A proposed framework for Botnet Spam-email Filtering using Neucube." (2017), The International Arab Conference on Information Technology, Yassmine Hammamet, Tunisia, December 22-24, 2017.

[22] Mohammadzadeh, Hekmat, and Farhad Soleimanian Gharehchopogh. "A novel hybrid whale optimization algorithm with flower pollination algorithm for feature selection: Case study Email spam detection." Computational Intelligence (2020).

[23] Asif Karim, Sami Azam, Bharanidharan Shanmugam, Krishnan Kannoorpatti, Mamoun, Alazab, "A Comprehensive Survey for Intelligent Spam Email Detection." IEEE Access 7 (2019): 168261-168295.

[24] D. Hassan, "Investigating the Effect of Combining Text Clustering with Classification on Improving Spam Email Detection.", Advances in Intelligent Systems and Computing Intelligent Systems Design and Applications, 99-107. doi:10.1007/978-3-319-53480-0_10, 2017.

[25] H. Padhiyar and P. Rekh, "An Improved Expectation Maximization based Semi-Supervised Email Classification using Naïve Bayes and K- Nearest Neighbor.", International Journal of Computer Applications, vol. 101, no. 6, pp. 7–11, 2014.