Spam Detection by Machine Learning Algorithms

Maruf Hasnat and S M Ibrahim Hossain

A Thesis in the Partial Fulfillment of the Requirements

For the Award of Bachelor of Computer Science and Engineering (BCSE)

Department of Computer Science and Engineering

College of Engineering and Technology

IUBAT – International University of Business Agriculture and Technology

Summer 2022

Spam Detection by Machine Learning Algorithms

Maruf Hasnat and S M Ibrahim Hossain

A Thesis in the Partial Fulfillment of the Requirements for the Award of Bachelor of Computer Science and Engineering (BCSE)

The thesis has been examined and approved,

____

Prof. Dr. Utpal Kanti Das

Chairman and Professor

____

Dr. Muhammad Hasibur Rashid Chayon

Co-supervisor, Coordinator and Associate Professor

____

Md Saidur Rahman

Assistant Professor

CSE Department, IUBAT

Department of Computer Science and Engineering

College of Engineering and Technology

IUBAT – International University of Business Agriculture and Technology

Letter of Transmittal

21 August 2022

The Chairman
Thesis Defense Committee
Department of Computer Science and Engineering
IUBAT–International University of Business Agriculture and Technology
4 Embankment Drive Road, Sector 10, Uttara Model Town
Dhaka 1230, Bangladesh

Subject: Letter of Transmittal.

Dear Sir,

It gives me enormous pleasure to work on “Spam Detection by Machine Learning Algorithms” as per instructions. We expect this research work to be informative as well as comprehensive.

While conducting the thesis paper we have gathered lots of knowledge about the spam detection by machine learning algorithms. We have tried my level best to collect the relative information as comprehensively as possible in preparing the thesis. During preparation of the research paper, we have experienced a lot that will help me greatly in my career. We will be able to explain anything for clarification if necessary.

We would like to thank you for giving me the opportunity to do a research work on the above Mention topic.

Yours sincerely,

_______________	_______________
Maruf Hasnat	S M Ibrahim Hossain
19103011	19103058

Student’s Declaration

We hereby declare that this thesis is based on results obtained from our own work. All the materials that were used for the purpose of completing this thesis are acknowledged and mentioned in reference. This thesis. Neither in whole nor in part, has been previously submitted to any other University or Institute for the award of any degree or diploma. We carried out our research under the supervision of Md Saidur Rahman.

Maruf Hasnat	S M Ibrahim Hossain
19103011	19103058

Supervisor’s Certification

This is to certify that the thesis report on “Spam Detection by Machine Learning Algorithms” has been carried out by Maruf Hasnat bearing ID#19103011 and S M Ibrahim Hossain bearing ID# 19103058 student of Department of Computer Science and Engineering, IUBAT-International University of Business Agriculture and Technology. The report has been prepared under my guidance and is a record of work carried out successfully. To the best of my knowledge and as per their declaration, no parts of this report has been submitted anywhere for any degree, diplomaor certificate. Now they are permitted to submit the report. I wish their success in their future endeavors.

Md Saidur Rahman

Assistant Professor

Department of Computer Science and Engineering

IUBAT–International University of Business Agriculture and Technology

Abstract

Now a days, we use many communication mediums like Short Message Service (SMS), Email, etc. Many times, we can see the text distinguish as spam. Spam is one type of text that is meaningless, unuseful, and unexpected to a receiver. Sometimes it can be a trap. Also, it can carry any kind of virus, malware, Trojan, etc. It wastes our time and space and sometimes can destroy our devices also. Spam slows down our organization's productivity by keeping our team busy with unnecessary tasks. It's true that it takes a long time to open a mailbox and delete all spam emails. Today, spam is one of the most common vectors for spreading threats, including malware. These seemingly harmless links and attachments can pose real threats to our business as they hide ransom ware, spyware and Trojan horses and give attackers access to our computer and even our entire corporate network. According to Verizon reports, it is said that approximately 94% of security breaches involving malware occur using malicious emails. Spam is often used for spoofing and phishing scams, but this can also be related to malware distribution. Spam is repeatedly happening because we don’t have an accurate method for spam detection. Spammers regularly update their technic. So sometimes it’s complicated to identify whether it is spam or not spam message. The popularity of communication media is increasing daily, and at the same time, the number of spamming activities is also growing. So, in this paper, we will filter spam and non-spamming text using modern machine learning algorithms to get efficient results for detecting all spam messages.

Keywords: spam, machine learning algorithms, LabelEncoder, Naïve Bayes, data preprocessing, Sklearn.

Acknowledgements

In the name of Almighty Allah who is the most merciful and most graceful. We would like to thank the late Professor Dr. Md. Alimullah Miyan, Vice-chancellor of IUBAT- International University of Business Agriculture & Technology gave us permission to study in this university which is the most beautiful and renowned, the first non –government university in this country.

We would like to thank and convey the respect to our present honorable vice chancellor Professor Dr. Abdur Rab, IUBAT- International University of Business Agriculture & Technology.

We would like to give gratitude to Prof. Dr. Utpal Kanti Das, chairman of Department of computer science and Engineering, IUBAT-International University of Business Agriculture & Technology, gave permission to study in the Department of Computer science & Engineering and allow us to see the bright future in the technological field of the new era.

We are very appreciative to Dr. Muhammad Hasibur Rashid Chayon respected co-ordinator and professor, Department of computer science & Engineering, IUBAT- International University of Business Agriculture & Technology, for his better direction and sustain throughout the semester.

We are really pleased and proud to express our feeling of gratefulness and profound respect to our respected faculty, Md Saidur Rahman Assistant Professor, Department of computer science & Engineering-IUBAT for his scholastic guidance, helpful and untiring efforts to execute our research work.

Finally, we would like to thank our parents and our teachers who have been a great source of inspiration to us.

Table of Contents

List of Figures

List of Tables

Chapter 1. Introduction

1.1 Introduction

Spam has a lot of definitions, but to make it easier, it defines the mass transmission of unwanted messages as spam. It has now become a major online problem. Spam accounted for 55% of all e-mail communications in 2017, the same as it did the previous year. Spam, also known as unsolicited bulk email, has increased the use of email because it provides a convenient way to send unwanted advertisements or junk newsgroup postings at no cost to the sender. This opportunity has been widely utilized by unscrupulous groups, resulting in the cluttering of millions of people's mail boxes all around the world.

Spam’s history can be traced back to 1864. The first unsolicited electronic message was probably telegraphed by him in 1864. These were suspicious investment proposals offered to rich Americans. The spam saga continued on May 3, 1978, when a guy called Gary Sark sent the first spam email. There, then working for Digital Computer Corp., sent an email request on the day of publication to present his new VAX computer to the company. ARPANET (a military computer network funded by DARPA and pre-Internet) email was sent to about 400 of the 2,600 people with his account.

Spam grows almost exponentially, eventually accounting for the majority (80-85%) of the 4,444 messages sent worldwide. Up to 182.9 billion email messages are sent and received worldwide every day (as of 2014). This is a long-running battle between spammers and just about everyone else. The technology and techniques used to send and block spam are advancing at an alarming rate the list continues on and on: email harvesting botnets, DMARC, zombie networks, neural network-based spam filters, domain-based message authentication, reporting, and compliance. According to Symantec Corporation's "2014 Internet Security Threat Report, Volume 19," the tide has recently swung in favor of spammers, with spam levels falling to (66% - 85%) of all email traffic. It's at a disadvantage. But this war isn't over yet.

Spam rarely comes directly from companies that advertise themselves. It is usually sent by "spammers", companies that distribute unwanted emails. Advertisers contract spammers to send email advertisements to groups of unsuspecting recipients. Spam costs much less than bulk mail. For less than $100, he can spam 10,000 recipients, whereas an advertiser costs thousands of dollars for a single email. How do spammers find you? In some cases, software programs called "harvesters" are used to purchase or obtain user addresses. This software program extracts the name of her website, newsgroup, or other service where the user identifies herself by her email address. Although not all spam text messages are frauds, they are frequently. Scammers will tell you a variety of stories in order to fool you. This messages include:

- You've been offered a credit card with no or low interest.
- You have won a reward, a gift card, or a voucher that you must use.
- There is a notice concerning a delivery package, maybe requesting you to accept it.
- Your account has been disabled for your safety, and you must take the necessary actions to reinstate it.
- You were overcharged and are entitled to a reimbursement from a government agency such as the IRS or HMRC.
- You can obtain aid paying off your school loans.

- You may delete unfavorable information from your credit report for a cost.
- There is an issue with your payment information; you must take action.
- Suspicious activity has been detected on your account, and you must take additional action.

In-case of fake text messages, these messages often try to create a sense of urgency. For example, claiming 'Need urgent attention' or 'Reply within 2 days'. The messages typically ask for personal information such as bank and card details, social security numbers, etc., in order to claim a gift or pursue an offer. You may be asked to confirm. Clicking on the link will take you to his fake website, and once you sign up, the scammer can steal your credentials. Other types of SMS spam might inadvertently install malware on your electronic devices, stealing your personal information.

According to our idea, we will use different types of machine learning algorithms to detect spam messages. By seeing the accuracy and precision, we will decide which algorithm or model will detect better for detecting spam messages. With a mix of integrated and complementary data encryption and storage technologies, as well as a platform for the representation and use of open and scalable data, the concept might be particularly creative in the consumer cyber security arena. So, based on the accuracy and precision, we will differentiate the machine algorithms and also try to understand what type of messages are called spam and not spam. These will create an awareness among the users about spam messages and make their privacy safe. So, to understand which machine learning algorithm works better for spam detection we need to train our datasets, test it and see the results.

The following is how the paper is organized: The second section provides an overview of related studies. In Section 3, we outline our strategy. Finally, Section 4 contains the findings, results, and discussion, as well as some rationale concerning our study.

1.2 Motivation

Spam blocks communication channels and generates traffic that providers or users (or employers in the case of businesses) have to pay for. According to Alexander Ivanov, head of the Russian Association of Networks and Services, the Internet operator lost $55 million due to spam damage three years ago. This number alone represents the cost of traffic. There are also mail servers that receive and process spam, and these servers must be maintained by highly paid professionals. Thus, significant infrastructure operating costs also occur. If spam arrives in a user's inbox, the recipient must manually delete it. A person who reads 10-20 of his or her emails in a day can receive approximately 160-180 spam messages along with business correspondence. That means he or she spends 5-6 hours a month just deleting spam, at the expense of productive work hours. The need to manually remove spam makes the user a processing engineer for "electronics". Forcing such behavior only frustrates the user and leads to unwanted and negative emotions. Losing essential emails by accidentally deleted along with mass spam. Anyone who has faced such a situation will immediately understand. No further comments are needed.

So, to address these challenges, we shall employ several sorts of machine learning techniques. These algorithms use statistical models to classify data. Spam detection requires a trained machine learning model to be able to determine if a phrase found in an email is similar to a phrase found in spam email or a safe phrase. So, on the basis of accuracy and precision we will decides which algorithm performs better for detecting spam messages. Overall, by detecting spam messages we can save our personal and business privacy from any spammers.

1.3 Problem statement

Spammers and spam filters are in a fierce rivalry every day as spammers try cunning tactics to get past the spam filters, such as adding strange characters to the subject line or sending emails with random sender addresses. The lack of machine learning emphasizes the creation of models that can forecast activity. Since the user must go through the undesirable junk mail and use up storage space and communication bandwidth, spam is a time waster for the user. It is difficult to manually compare the correctness of classified data since rules in other existing systems must be continuously updated and maintained, adding to the strain on some users.

1.4 Objective

The detection of spam is a significant problem in mobile SMS communication, which makes it insecure. A precise and accurate mechanism for detecting spam in mobile SMS communication is required to address this issue. For specific identification, we suggested using machine learning-based spam detection techniques. There are four goals that must be met for this project:

i. Researching spam detection methods using machine learning.

ii. To modify the computer system environment for the machine learning algorithm.

iii. Appling the best machine learning algorithm knowledge for analyzing software.

iv. Dataset of spam messages from Kaggle is used to evaluate the machine learning algorithm.

Chapter-2 Literature Review

2.1 Literature Review

This chapter offers a study of the literature regarding machine learning classifiers that have been employed in prior studies and projects. It is not about obtaining information, but rather about summarizing previous research relevant to this issue. It entails seeking, reading, analyzing, summarizing, and assessing. The project-related reading materials According to literature reviews on the issue of machine learning, the majority of spam Filtering and detecting algorithms must be taught and updated on a regular basis. For spam filtering to operate, rules must also be set. As a result, it gradually became a strain on the user.

2.2 RELATED WORK

The majority of research has been on spam text filtering and detection utilizing a number of strategies. Thiago S. Guzella and colleagues conducted a review of spam filtering machine learning methods (2009). They observed in their article that Bayesian Filters, which are used to filter spam, needed a significant training time before they could perform successfully.

S. Ananthi (2009) conducted a review of "spam filtering Using K-NN" She chose one of the most basic fundamental algorithms that are KNN algorithms. When the class is small, the categorization of an item is chosen by the majority vote of its neighbors.

Michael Crawford, Michael Crawford, Taghi M. Khoshgoftaar, Joseph D. Prusa, Aaron N. Richter & Hamzah Al Najada (2015) conducted a review of the Survey of review spam detection using machine learning techniques. They basically work for filtering Opinion (Review) Spam. They aruse Natural Language Processing (NLP).

Shirani-Mehr, H. (2013) reviewed "SMS Spam using Machine Learning Approach".He said on that paper that 30% of text messages were unwanted which means spam in 2012. Also, he determined that we do have not enough data in the database to identify the unwanted text or spam. After using SVM as the learning algorithm he got an accuracy of 97.64% and after boosting naïve Bayes overall accuracy is 97.50.

Machine Learning study Classifiers for Spam Detection conducted by "Shrawan Kumar Trivedi". He first observed some of the machine learning classifiers such as J48 (Decision Tree), Bayesian with Adaboost, SVM (support vector machine) etc. Among all of the models he chose the SVM. Because SVM gives more accurate results than any other model. But one of the problems of SVM (Support vector machine) take much time.

Simon Tong and Daphne Koller (2001) investigated "Support Vector Machine Active Learning with Applications to Text Classification." They presented a new algorithm for active learning with SVM induction and transduction in this paper. It is used to minimize version space as much as possible at each query. They discovered that the existing dataset differed from the original labelled data set by only one instance.

According to a research undertaken by Naeem Ahmed [2021] and his colleagues, the majority of suggested IoT and email spam detection systems are based on machine learning methodologies.

They basically want so say that email can contain 2 subcategories (ham and spam). Spam is also called junk text or unwanted text. They are observed several machine learning algorithm like Naïve Bayes, decision trees, neural networks, and random forest. Based on precision, recall they made a comparison and future research directions are also discussed.

According to Nandhini.S and Dr.Jeen Marseline.K.S [2020], the majority of suggested Performance Evaluation of Machine Learning Algorithms for Email Spam Detection. Their work they use weka tool for training and testing data sets. And their used database is UCI Machine learning Repository spam base data set. They used five important machine learning classification algorithm, Logistic Regression, Decision Tree, Naïve Bayes, KNN and SVM for filtering unwanted text (spam).Result show that random forest decision tree performance is better than any other machine learning classification algorithm. Although KNN machine learning classification algorithm give same result but it took more time to build.

Dr. Aaisha Makkar and her colleagues conducted a review of spam filtering for IoT Devices using Machine Learning. In their paper using machine learning for detecting IoT devices spam .They proposed a framework .That framework contain five machine learning models. And they set a comparison between all of the model. The use REFIT Smart Home database for validation for proposed technique.

According to Nikhil Govil , Kunal Agarwal and their colleagues [2020] the majority a machine learning based spam detection mechanism. In their paper they presented one tactic by which can filter spam and non-spam emails. Their suggested approach creates a dictionary as well as features. Machine learning is used to train them for effective results.

This chapter detailed the approach and model employed in the proposed project.

The approach and model are chosen based on existing research publications and journals. Every model’s benefits and drawbacks are exposed here.

Chapter-3 Research Methodology

3.1 Selecting a Dataset

A dataset is a grouping of different kinds of data that has been digitally preserved. Any project using machine learning needs data as its primary input. Datasets are largely composed of photos, texts, sounds, videos, numerical data points, etc., and are used to address a variety of AIdifficulties, including detecting objects, categorization of images or videos, face identification, classifying emotions, linguistic analysis etc. In our case we are selecting our datasetof spam messages from Kaggle which allows users to collaborate with other users, find and publishdatasets, use GPU integrated notebooks, and compete with other data scientists to solve data science challenges. This dataset includes a single batch of 5,574 English messages that have beenclassified as spam or ham (genuine) messages.

3.2 Feature Extraction

For deep learning and machine learning, feature extraction is very important. The technique of turning raw data into numerical features that can be handled while keeping the information in the original data set is known as feature extraction. Compared to using machine learning on the raw data directly, it produces better outcomes. After choosing a dataset, we then recognize and extract the features from it. The methodology's most crucial step is this one. Categorical features in the spam dataset must be converted to numbers or boolean values. Here, we will use LabelEncoder from Sklearn. A very effective method for converting the levels of categorical features into numerical values is offered by Sklearn. Labels with values between 0 and n classes-1, where n is the number of different labels, are encoded by LabelEncoder. If a label appears more than once, the previous value is assigned when it does. Here, we will assign ham (genuine) messages as value 0 and spam messages as value 1 by LabelEncoder from Sklearn for feature extraction.

3.3 Feature Selection

With the use of just relevant data and the elimination of irrelevant data, feature selection is a technique for lowering the input variable for our model. It involves automatically selecting features for our machine learning model that are important to the problem we are attempting to solve. By choosing the most crucial variables and removing redundant and irrelevant features, feature selection enhances machine learning and boosts the prediction power of machine learning algorithms. To choose features from the retrieved ones, this step is necessary. In order to minimize the size of the input training matrix, feature selection approaches are used. Here we are keeping v1 and v2 columns from datasets of spam messages where v1 column is containing ham (genuine) and spam messages and v2 column is containing the texts or messages and after that we remove other unused or unuseful columns to minimize the size of the input training matrix. After removing the unnecessary columns, we are renaming the v1 column as target column which is containing ham (genuine) and spam messages and the v2 column as text column which is containing the texts or messages.

3.4 Data Preprocessing

Preparing raw data to be acceptable for a machine learning model is known as data preparation. In order to build a machine learning model, it is the first and most important stage. It is not always the case that we come across the clean and prepared data when developing a machine learning project. Data preprocessing is necessary to clean the data and prepare it for a machine learning model, which also improves the model's accuracy and effectiveness. Here we will do data preprocessing by following some tactics like lower case, tokenization, removing special characters, removing stop words and punctuation, stemming etc.

Lower case means changing a word from upper case to lower case (ML to ml). Even if terms like "Book" and "book" have the same meaning when written in lower case, the vector space model represents them as two distinct words. Tokenization is the division of text into a collection of meaningful fragments. These objects are known as tokens. For instance, we could break up a passage of text into words or phrases. Removing special characters, stop words and punctuation will minimize the complexity of the text or messages. The process of stemming entails creating morphological variations of a root or base word. Stemmers or Stemming algorithms are other names for stemming programs. Stemming reduces a word to its lemma, which is the root of a word that includes suffixes, prefixes, and other affixes.

3.5 Comparison of Algorithms

Making sure that all machine learning algorithms are evaluated uniformly on the same set of data is essential for conducting a fair comparison of them. This can be done by requiring that each algorithm be tested using a uniform test harness. We wanted to compare eleven chosen algorithms. In this step, a variety of machine learning models must be trained, including: Logistic Regression, Support Vector Classifier (SVC), Multinomial Naïve Bayes, Decision Tree Classifier, K-Neighbors Classifier, AdaBoost Classifier, Bagging Classifier, Random Forest Classifier, Extra-Trees Classifier, Gradient Boosting, and Extreme Gradient Boosting (XGB) Classifier.

3.6 Spam Detection

In this step, we are testing our model to check if it can accurately identify spam messages from the spam messages dataset constitutes the implementation step. The accuracy and precision score of the aforementioned models are used to calculate the spam detection system's overall performance.

3.7 Process Model

A process model is a list of actions, each with a clear description and associated choices that must be made in order to complete the project execution. The project flows must be followed in order to complete the project in the allotted time. The project's general flow is depicted in the structure below, which demonstrates how to distinguish between spam and legitimate messages.

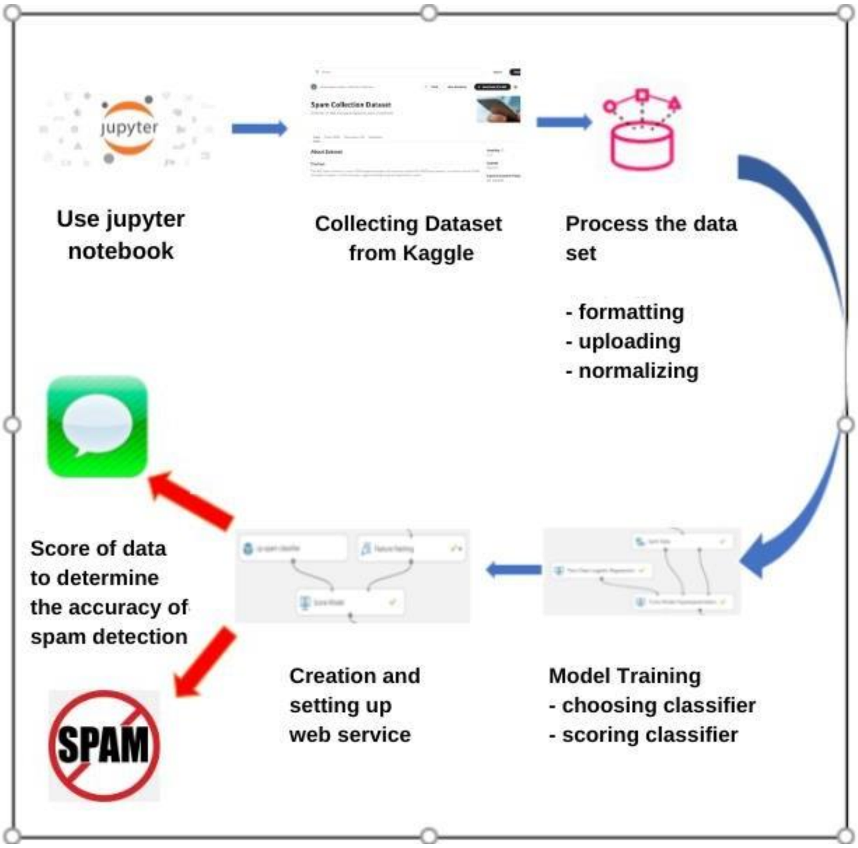


Fig 3.1: Process framework

3.8 Data Model

The term "data model" describes the process of describing a complex system's data flow between various data pieces and designing it as a simple, text-and-symbol diagram. The data flow below demonstrates how these projects' data flow in order to identify spam messages and categorize them into two distinct types, namely spam and ham communications.

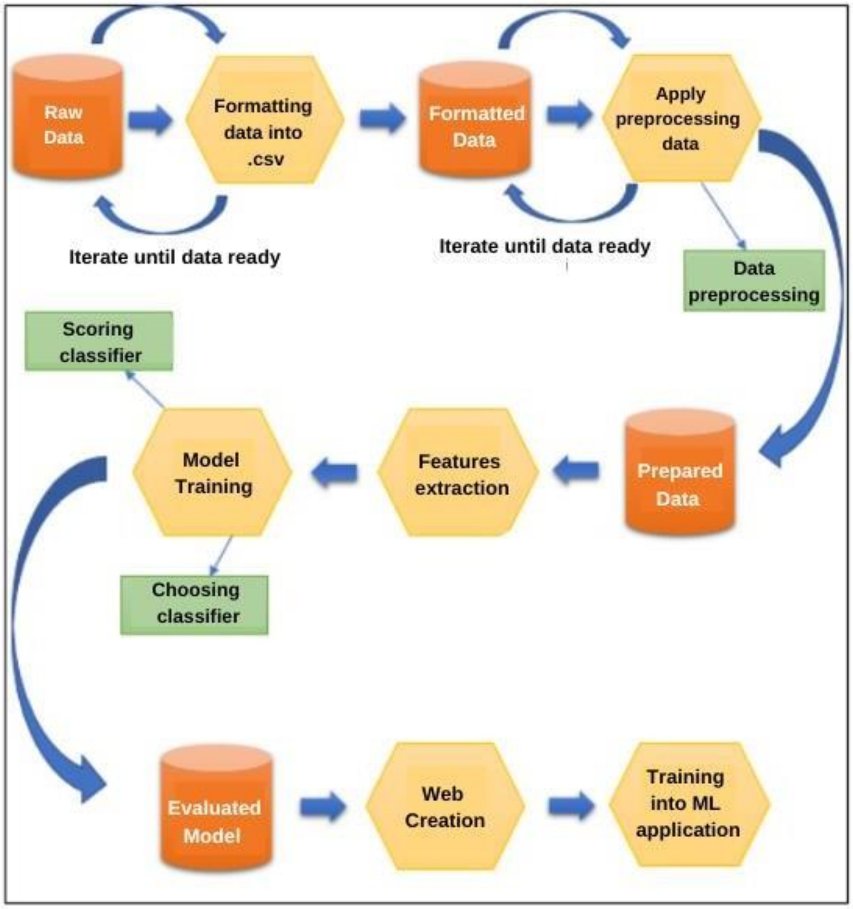


Fig 3.2: Data model flow

Chapter-4 Result & Discussion

The implementation and testing of the project will be covered in this chapter. The last phase of project development includes both the implementation and testing outcomes. Verifying that the project development was a trained model to meet the requirement requires implementation. The testing outcome is a demonstration of the steps used to guarantee the functionality of the final product.

At this stage, it will demonstrate how effectively the machine learning model is working and identify any areas that need improvement. Thus, when the project has been established, this chapter will normally address its implementation, deployment, and testing.

4.1 Data Visualization

This is the outcome of a pie chart that shows the percentages of spam and ham, with spam coming in at 12.63% and ham at 87.37%. This pie chart, which closed with the message length, estimated the fraction of the data that is spam or ham. We can understand by seeing the chart that data is imbalanced.

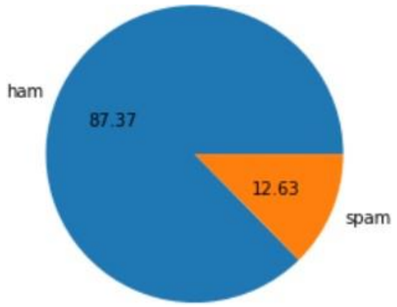


Fig 4.1: Pie chart in Percentage

Here we can see the common words which are used rapidly in spam messages. There are the spam words that are categorized as being used the most frequently.

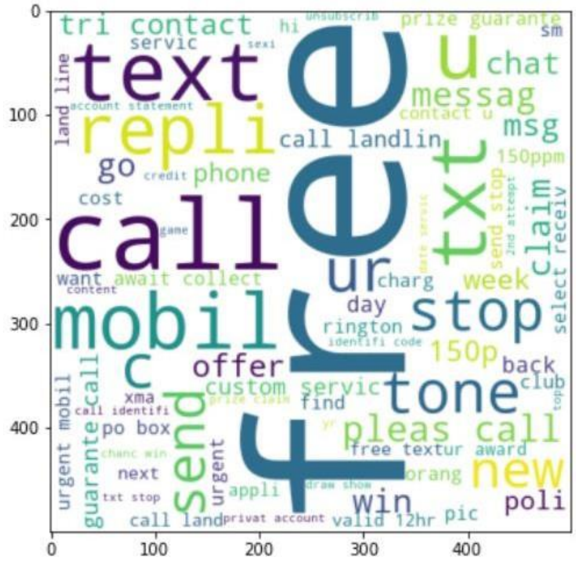


Fig 4.2: Spam words list

Here we can also the common words which are used rapidly in ham messages. The words that are detected as ham the most frequently appeared on this list.

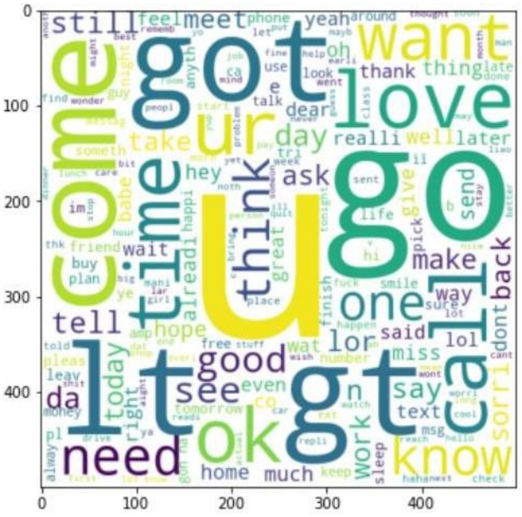


Fig 4.3: Ham words list

4.2 Algorithm’s Accuracy and Precision

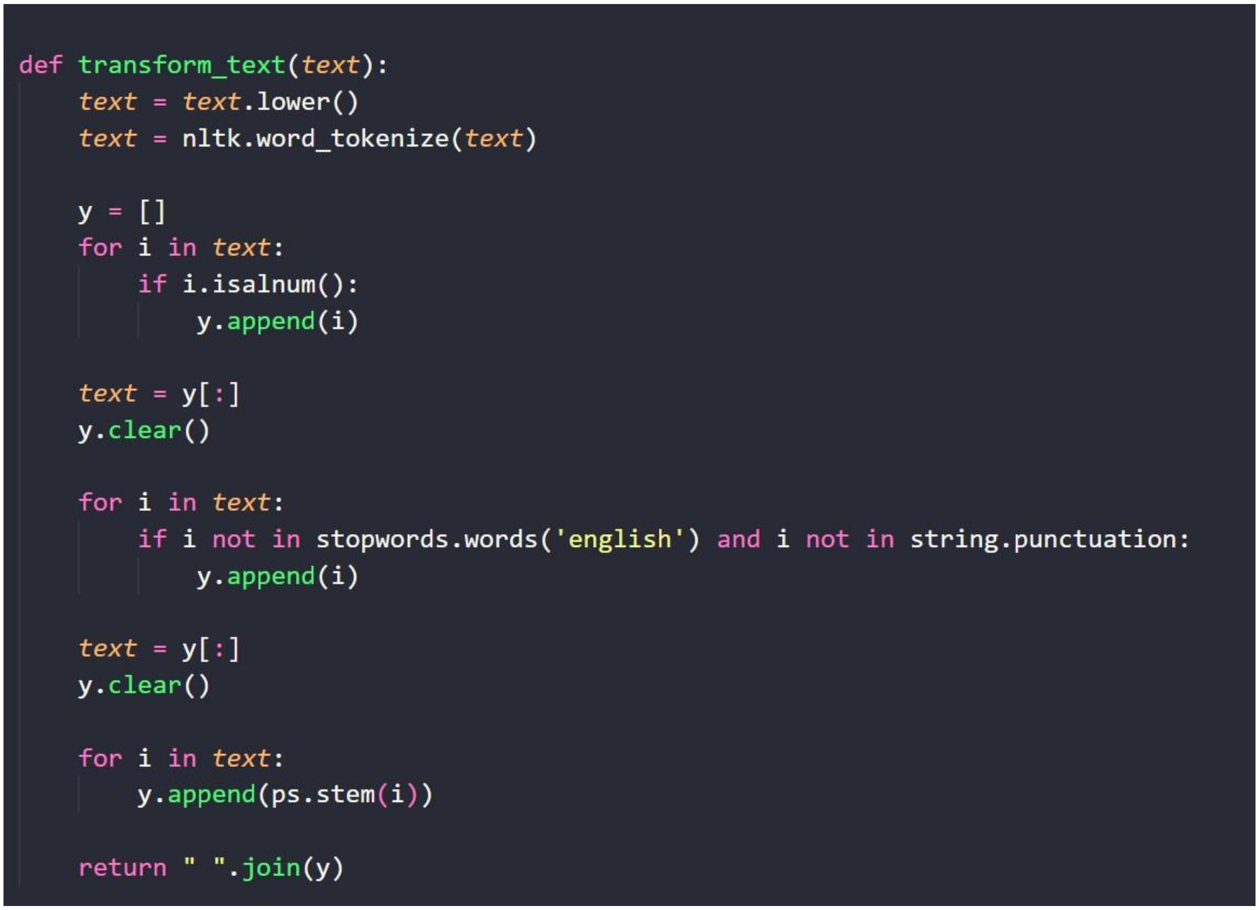
No.	Algorithms	Accuracy	Precision
1	Logistic Regression	0.958414	0.970297
2	Support Vector Classifier (SVC)	0.975822	0.974790
3	Naïve Bayes	0.970986	1.000000
4	Decision Tree Classifier	0.932302	0.833333
5	K-Neighbors Classifier	0.905222	1.000000
6	AdaBoost Classifier	0.960348	0.929204
7	Bagging Classifier	0.958414	0.868217
8	Random Forest Classifier	0.975822	0.982906
9	Extra-Trees Classifier	0.974855	0.974576
10	Gradient Boosting	0.946809	0.919192
11	Extreme Gradient Boosting (XGB) Classifier	0.967118	0.933333

Table 4.1: Different algorithm’s accuracy and precision

Here we can see the accuracy and precision of different machine learning algorithms. As we are focusing more on precision, so we are selecting Naïve Bayes algorithm for web-based implementation to detect spam messages. Although Random Forest has good accuracy and precision score but as Naïve Bayes has 100% precision, so we are choosing the algorithm for detecting spam messages in web-based system.

4.3 Implementation

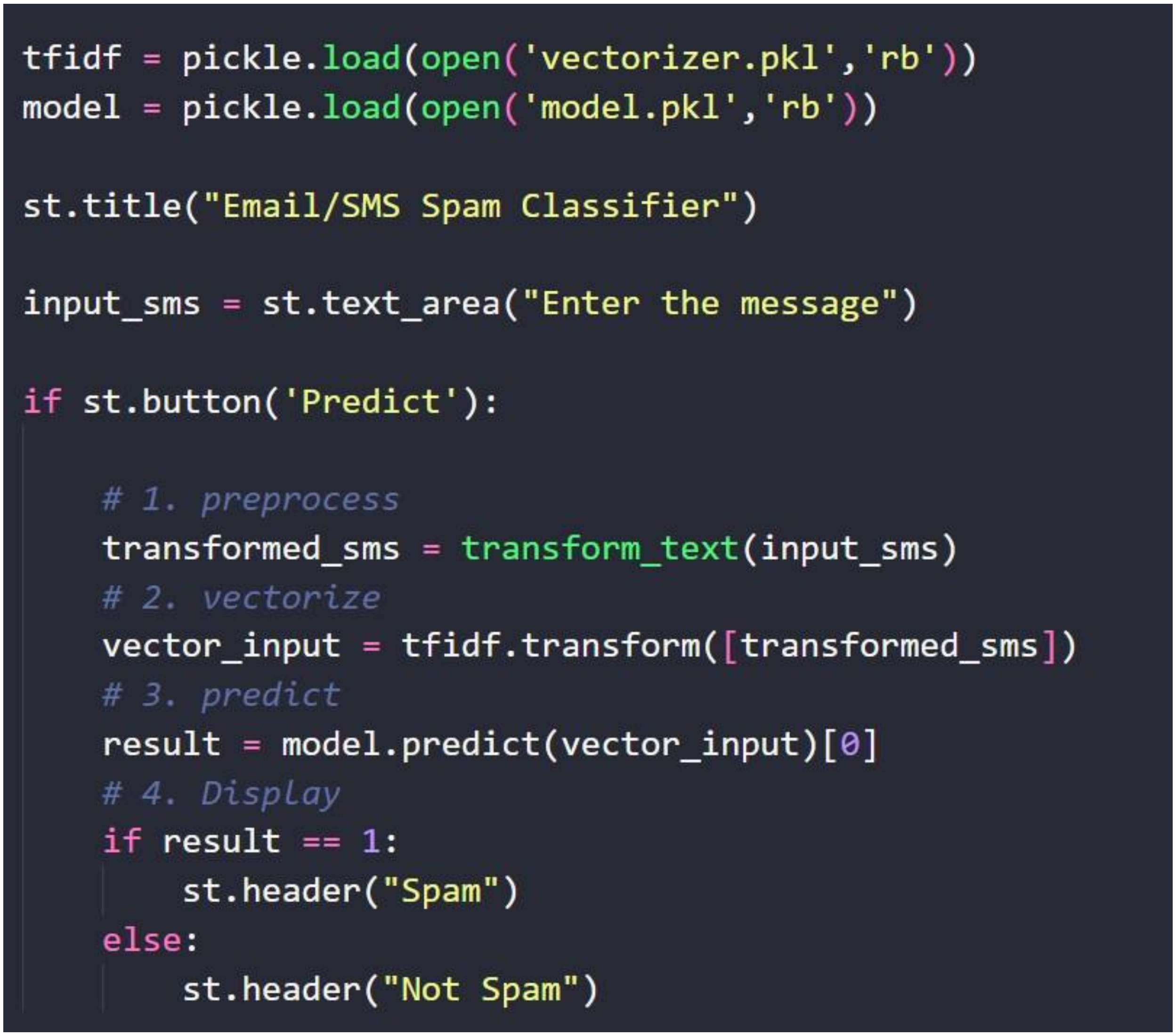
Here we will use python framework Streamlit for web-based implementation. We will use Visual Studio Code as code editor for writing codes. In Visual Studio Code, we will write our logic for detecting the spam messages. First, we will simplify the message by our logic.



```
def transform_text(text):
    text = text.lower()
    text = nltk.word_tokenize(text)

    y = []
    for i in text:
        if i.isalnum():
            y.append(i)

    text = y[:]
    y.clear()

    for i in text:
        if i not in stopwords.words('english') and i not in string.punctuation:
            y.append(i)

    text = y[:]
    y.clear()

    for i in text:
        y.append(ps.stem(i))

    return " ".join(y)
```

Fig 4.4: Simplifying messages

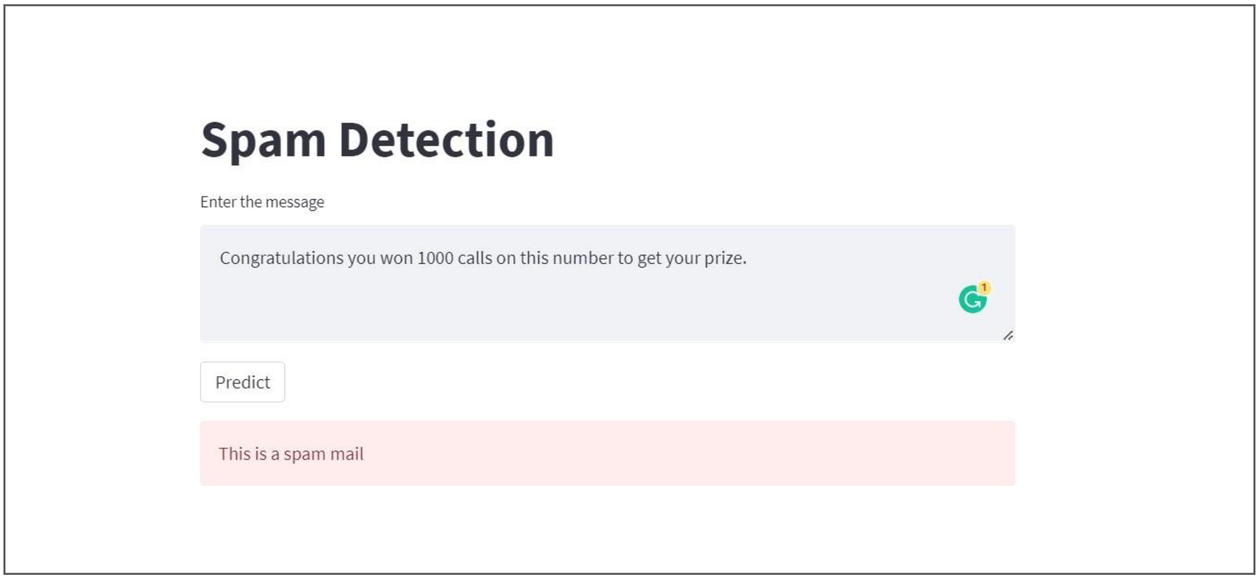
Then, we will apply our Naïve Bayes algorithm model on simplified message to detect spam messages easily.



```
tfidf = pickle.load(open('vectorizer.pkl','rb'))
model = pickle.load(open('model.pkl','rb'))

st.title("Email/SMS Spam Classifier")

input_sms = st.text_area("Enter the message")

if st.button('Predict'):

    # 1. preprocess
    transformed_sms = transform_text(input_sms)
    # 2. vectorize
    vector_input = tfidf.transform([transformed_sms])
    # 3. predict
    result = model.predict(vector_input)[0]
    # 4. Display
    if result == 1:
        st.header("Spam")
    else:
        st.header("Not Spam")
```

Fig 4.5: Applying model

Finally, we will run the python file which contains the code for spam detection by Streamlit command in terminal or command prompt and can see the interface and can also detect any message whether that message is spam or ham (not spam).

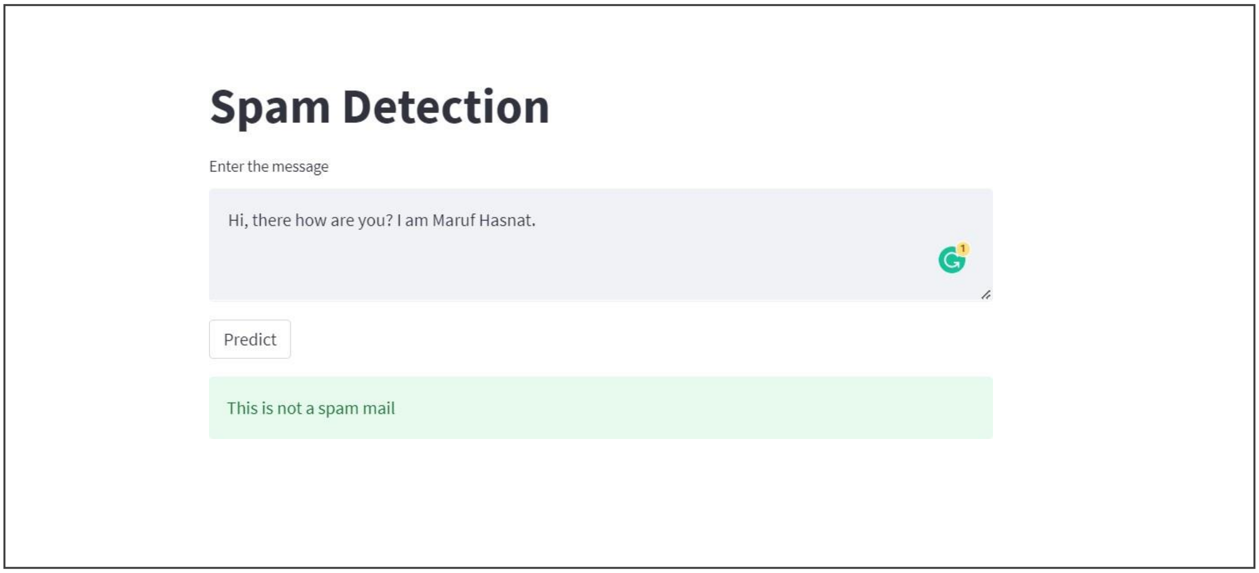

Spam Detection

Enter the message

Congratulations you won 1000 calls on this number to get your prize.

This is a spam mail

Fig 4.6: Interface for detecting spam messages


Spam Detection

Enter the message

Hi, there how are you? I am Maruf Hasnat.

This is not a spam mail

Fig 4.7: Interface for detecting ham (not spam) messages

Chapter 5. Conclusion

5.1 Conclusion

We had seen that supervised ML is effective at interpreting messages and classifying them into the appropriate groups. Additionally, it can successfully specify the types of messages to be sent.For instance, the messaging interface keeps its users tricked by employing the naive Bayes methodbased on ML software. Only text (communications) and certain terms can be identified as spam orham messages based on the outcomes of this research. This project does not block messages; it simply focuses on message detection, analysis, and classification. One recommendation for this project is to use it for more than just categorizing text message formats. Therefore, it is possible toenhance this project's use so that it can identify, analyze, and classify models for any format, suchas a spam word cloud, in addition to merely text messages. These enhancements must be done if we want to classify objects with the greatest accuracy. It is clear from this study that Kaggle Machine Learning is a cloud-based collaborative tool with the ability to find analytical solutions for specific types of data. In order to identify spam, this research made use of the Python-based Kaggle Machine Learning algorithm. Based on the presented dataset, the classification method inNaive Bayes has been utilized to identify spam or ham. The accuracy of the data source has an impact on categorization performance. Data with redundant and irrelevant attributes could make detection less accurate. Only text (messages) can be categorized and used to identify spam or hammessages during implementation. This project does not attempt to prevent messages; it primarily focuses on detecting, analyzing, and classifying them. Thus, the proposed methodology may be used to improve upon the shortcomings of the current spam detection methods. From this study, itcan be stated that one of the key components in developing applications for identifying spam is the machine learning algorithm. Future improvements must be made in order to increase efficiency.

5.2 Limitation of work

There are some limitations of this project work. This project is solely capable of detecting and calculating the accuracy of spam messages. It focuses on filtering, analyzing, and categorizing communications. The project does not block the spam messages.

5.3 Future work

In future we will try to make a system which will basically capable of blocking the spam messages and notify the user about the spam messages which will help the user to identify about the spam messages and know the source of spam messages.

References

[1] Crawford, M., Khoshgoftaar, T.M., Prusa, J.D., Richter, A.N. and Al Najada, H., 2015. Survey of review spam detection using machine learning techniques. Journal of Big Data, 2(1), pp.1-24.

[2] Shirani-Mehr, H., 2013. SMS spam detection using machine learning approach. unpublished) http://cs229.stanford. edu/proj2013/Shir aniMeh r-SMSSpamDetectionUsingMachineLearning Approach. pdf.

[3] Trivedi, S.K., 2016, September. A study of machine learning classifiers for spam detection. In 2016 4th international symposium on computational and business intelligence (ISCBI) (pp. 176-180). IEEE.

[4] Ahmed, N., Amin, R., Aldabbas, H., Koundal, D., Alouffi, B. and Shah, T., 2022. Machine learning techniques for spam detection in email and IoT platforms: analysis and research challenges. *Security and Communication Networks*, *2022*.

[5] Guzella, T.S. and Caminhas, W.M., 2009. A review of machine learning approaches to spam filtering. *Expert Systems with Applications*, *36*(7), pp.10206-10222.

[6] Govil, N., Agarwal, K., Bansal, A. and Varshney, A., 2020, March. A machine learning based spam detection mechanism. In *2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC)* (pp. 954-957). IEEE.

[7] Awad, W.A. and ELseuofi, S.M., 2011. Machine learning methods for spam e-mail classification. *International Journal of Computer Science & Information Technology (IJCSIT)* , *3*(1), pp.173-184.

[8] Makkar, A., Garg, S., Kumar, N., Hossain, M.S., Ghoneim, A. and Alrashoud, M., 2020. An efficient spam detection technique for IoT devices using machine learning. IEEE Transactions on Industrial Informatics, 17(2), pp.903-912.

[9] Nandhini, S. and KS, J.M., 2020, February. Performance evaluation of machine learning algorithms for email spam detection. In 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE) (pp. 1-4). IEEE.

[10] Ahmed, N., Amin, R., Aldabbas, H., Koundal, D., Alouffi, B. and Shah, T., 2022. Machine learning techniques for spam detection in email and IoT platforms: analysis and research challenges. Security and Communication Networks, 2022.