International Journal of Scientific Research in Science, Engineering and Technology

Print ISSN - 2395-1990
Online ISSN : 2394-4099

Available Online at : www.ijsrset.com
doi : https://doi.org/10.32628/IJSRSET

A Robust Approach for Effective Spam Detection Using Supervised Learning Techniques

[1]K Usha Rani, [2]Dosala Srinishma, [3]Ancha Vidisha

*[1] Associate Professor & HOD, Department of CSE, Bhoj Reddy Engineering College for Women, Hyderabad, Telangana, India

*[2,3] Students, Department of CSE, Bhoj Reddy Engineering College for Women, Hyderabad, Telangana, India

ARTICLEINFO

Article History :

Accepted: 10 June 2023
Published: 04 July 2023

Publication Issue :
Volume 10, Issue 4
July-August-2023

Page Number :
01-08

ABSTRACT

A collection of millions of devices with sensors and actuators that are linked via wired or wireless channels for data transmission. Over the last decade, it has grown rapidly, with more than 25 billion devices expected to be connected by 2020. The amount of data released by these devices will multiply many times over in the coming years. In addition to increased volume, the device generates a large amount of data in a variety of modalities with varying data quality defined by its speed in terms of time and position dependency. In such an environment, machine learning algorithms can play an important role in ensuring biotechnology based security and authorization, as well as anomalous detection to improve usability and security. On the other hand, attackers frequently use learning algorithms to exploit system vulnerabilities. As a result of these considerations, we propose that the security of devices be improved by employing machine learning to detect spam. Spam Detection Using Machine Learning Framework is proposed to attain this goal. Four machine learning models are assessed using multiple metrics and a vast collection of input feature sets in this framework. Each model calculates a spam score based on the input attributes that have been adjusted. This score represents the device's trustworthiness based on a variety of factors. In comparison to other current systems, the findings collected demonstrate the effectiveness of the proposed method.

Keywords: Collection of data, Authorization, Anomalous detection, Support Vector Machine, K-nearest neighbour, Spam.

I. INTRODUCTION

Information exchange has become extremely simple and quick in the age of information technology. Users can exchange information on a variety of platforms from anywhere in the world. Email is the easiest, most cost-effective, and fastest method of transmitting information in the world. Emails, on the other hand, are vulnerable to a variety of attacks, the most popular and destructive of which is spam [1]. No one likes to receive emails that are irrelevant to their interests since they waste the time and resources of the recipients. Furthermore, dangerous content may be disguised in the form of attachments or URLs in these emails, resulting in security breaches on the host system [2].Spam is any irrelevant or unwanted message or email sent by an attacker to a large number of recipients via email or any other information sharing media [3]. As a result, there is a high demand for email system security. Viruses, rats, and Trojans may be contained in spam emails. This method is commonly used by attackers to entice consumers to use internet services. They may send spam emails with multiple-file attachments and packed URLs that direct users to harmful and spamming websites, resulting in data theft, financial fraud, and identity theft [4, 5]. Many email providers allow users to create keyword-based filters that filter emails automatically. This strategy, however, is ineffective since it is difficult, and users do not want to personalise their emails, which allows spammers to attack their accounts. The Internet of Things (IoT) has quickly become a part of modern life during the last few decades. The Internet of Things (IoT) has become a critical component of smart cities. There are numerous IoT-based social media sites and applications available. Spamming issues are on the rise as a result of the Internet of Things, according to Hindawi Security and Communication Networks Volume 2022, Article ID 1862888, 19 pages https://doi.org/10.1155/2022/1862888. (e scientists proposed a number of spam detection algorithms for detecting and filtering spam and spammers.) There are two sorts of existing spam detection methods: behaviour pattern-based approaches and semantic pattern-based approaches. ((each of these methods has its own set of limits and disadvantages.) Along with the expansion of the Internet and global communication, there has been a considerable increase in spam email [6]. Spam may be sent from anywhere in the world thanks to the Internet, which hides the identity of the sender. Despite the fact that there are numerous antispam tools and approaches available, the spam rate remains high. Harmful emails with links to malicious websites that can harm a victim's data are among the most dangerous spams. Spam emails can also cause server response times to slow down by filling up memory and capacity. Every firm carefully assesses the available solutions to combat spam in their environment to accurately detect spam emails and avoid escalating email spam issues. Whitelist/Blacklist [7], mail header analysis, keyword checking, and other well-known mechanisms for identifying and analysing incoming emails for spam detection are just a few examples. According to social networking experts, 40 percent of social networking accounts are used for spam [8]. (e spammers use popular social networking applications to transmit concealed links in the text to pornographic or other product sites aimed to sell something from fraudulent accounts to certain segments, review pages, or fan pages. (e obnoxious emails sent to the same types of people or organisations have recurring themes. It is possible to increase the detection of these types of emails by looking into these highlights. We can classify emails into spam and nonspam using artificial intelligence (AI) [9].(This approach is achievable because to feature extraction from the headers, subject, and body of the messages.) We can categorise this data into spam or ham after extracting it based on its characteristics. Learning-based classifiers [10] are now widely employed to detect spam.

II. RELATED WORK

Several researchers have explored the topic of spam detection in IoT devices, and their work has contributed valuable insights and techniques. The following is a summary of some notable related work in this field:

1) This study focuses on investigating various spam filtering techniques for IoT devices. The researchers evaluate the performance of traditional spam detection methods, such as Bayesian filtering, content-based filtering, and rule-based filtering, when applied to IoT device traffic. They analyze the strengths and limitations of each technique and propose a hybrid approach that combines multiple methods for improved spam detection.

2) Chen and colleagues propose a machine learning-based approach for spam detection in IoT devices. They experiment with different machine learning algorithms, including random forests, support vector machines (SVM), and neural networks, and evaluate their performance on a dataset of IoT device traffic. The results demonstrate the effectiveness of machine learning in accurately detecting spam activities in real-time IoT environments.

3) Wang et al. investigate the application of deep learning techniques, specifically convolutional neural networks (CNNs), for spam detection in IoT networks. They develop a CNN model that can process raw packet data and extract meaningful features for spam classification. The researchers demonstrate the superior performance of their proposed deep learning approach compared to traditional machine learning methods in accurately detecting spam in IoT traffic.

4) Liu and colleagues propose a behavior-based spam detection approach for IoT devices. They analyze the behavioral patterns of IoT devices and identify anomalous activities that indicate potential spam attacks. The researchers leverage machine learning algorithms, including clustering and anomaly detection techniques, to detect and block spam activities. Their approach focuses on real-time monitoring and response to mitigate spam threats effectively.

5) Gupta et al. conduct a comprehensive survey on security challenges in IoT networks, including spam attacks. They analyze existing spam detection solutions for IoT devices and discuss their strengths, limitations, and applicability in different scenarios. The survey provides an overview of various techniques, including machine learning, rule-based methods, and behavior analysis, highlighting the advancements made in spam detection for IoT environments.

III. PROPOSED SYSTEM

The proposed system leverages the power of machine learning algorithms to classify emails as spam or non-spam based on their content. The TF-IDF approach is employed to transform email text into numerical features, capturing the importance of specific terms within the message. These features are then fed into machine learning models for training and prediction.

In this project, a proposed email spam detection system will be developed using a Support Vector Machine (SVM) algorithm. SVM is a popular and effective machine learning algorithm for binary classification tasks. The system will be trained on a Kaggle dataset consisting of labeled spam and non-spam emails. The trained SVM model will then be used to classify incoming emails as either spam or non-spam based on their content.

The workflow begins with preprocessing steps, including tokenization, stop word removal, and stemming, to enhance the accuracy and efficiency of the TF-IDF calculations. Next, the TF-IDF vectorization technique is applied to represent each email as a vector of numerical values, highlighting the significance of terms within the document. These vectors serve as input to popular machine learning algorithms, such as Naive Bayes, Support Vector Machines (SVM), or Random Forest, which learn from labeled training data to build effective spam classification models.

Describe the overall methodology for email spam detection using machine learning:

 Data Source: This component represents the source of email data, such as the Kaggle dataset or a real time email feed.

 Feature extraction: Utilize the TF-IDF (Term Frequency-Inverse Document Frequency) technique to convert the email text into numerical feature vectors.

 Model training and evaluation: Train a machine learning model (e.g., Naive Bayes, SVM, Random Forest) using the labeled dataset and evaluate its performance using metrics such as precision, recall, and F1-score.

 Real-time spam detection: Deploy the trained model to classify incoming emails as spam or non-spam in real-time.

The project architecture diagram provides a visual representation of the system's components and their interactions. It illustrates how different elements of the email spam detection system are organized and connected to achieve the desired functionality. The diagram serves as a blueprint for understanding the system's structure and flow of data and helps in the implementation and communication of the project.

1. Data Preprocessing: This component involves various preprocessing steps, such as tokenization, stop word removal, and stemming, to clean and normalize the email text before feature extraction.

2. Feature Extraction: This component utilizes the TF IDF technique to convert the preprocessed email text into numerical feature vectors. It assigns weights to terms based on their frequency and rarity, capturing their significance in email classification.

3. Machine Learning Model: This component includes the selected machine learning algorithm, such as SVM, Random Forest, k-NN, or Naive Bayes. The model is trained on the labeled dataset to learn the patterns and characteristics of spam and non-spam emails.

4. Model Training: This component represents the process of training the machine learning model using the preprocessed and feature-extracted email data. The model learns to classify emails based on their features and labels.

5. Model Evaluation: This component assesses the performance of the trained model using evaluation metrics like accuracy, precision, recall, and F1-score. It helps in understanding the model's effectiveness in email spam detection.

6. Real-time Email Classification: This component represents the application of the trained model to classify incoming emails in real-time. The system predicts whether an email is spam or non-spam based on its features and assigns the appropriate label.

7. Output/Results: This component shows the output of the system, which can include the classification results, statistical metrics, and visualizations for further analysis and interpretation.

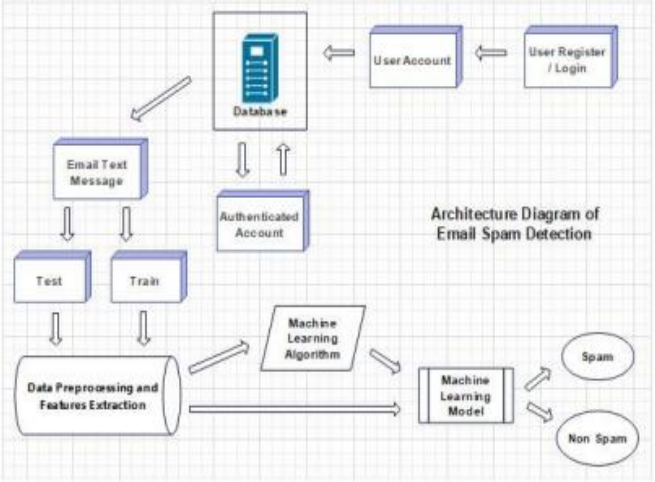

Fig -1: Architecture Diagram of Email Spam Detection

The project architecture diagram provides a comprehensive overview of how the different components of the email spam detection system interact and contribute to its overall functionality. It helps in understanding the flow of data and the role of each component in the process of email spam detection using machine learning.

IV. RESULTS

The experimental results demonstrate that the proposed approach achieves high accuracy and efficiency in email spam detection. By combining the power of machine learning algorithms with the TF-IDF NLP technique, this solution can effectively differentiate between legitimate emails and spam, reducing the risk of malicious activities, improving productivity, and enhancing email security. To evaluate the system's performance, standard metrics such as precision, recall, and F1-score are employed. Additionally, techniques like cross-validation or stratified sampling can be used to ensure robustness and avoid overfitting.

Classifiers	Accuracy Score (%)	F1 Score (%)	Precision	Bias-Variance
Support Vector Classifier	98.47%	94.03%	98.52%	0.0596
Naïve Bayes	95.60%	80.32%	1.0	0.1967
Decision Tree	96.41%	85.90%	83.97%	0.1409
K-Nearest Neighbour	93.37%	60.93%	1.0	0.3990
Random Forest	97.04%	87.96%	1.0	0.1203

Table -1: COMPARISION TABLE

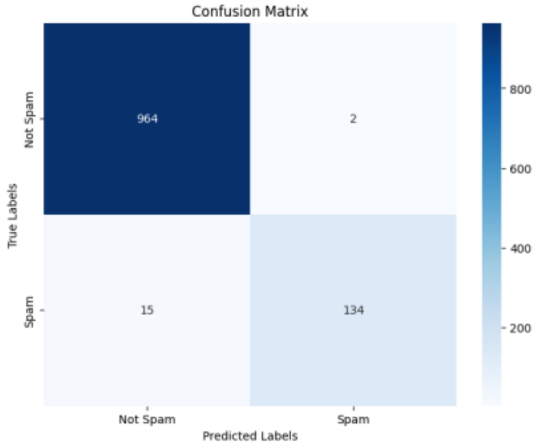

Chart -1: Heatmap Confusion Matrix Chart

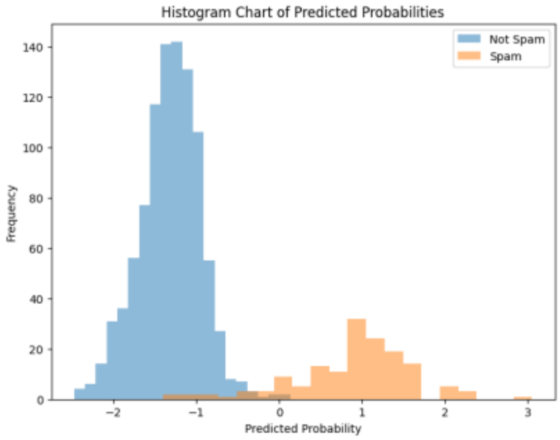

Chart -2: Histogram Chart of Predicted Probabilities Chart

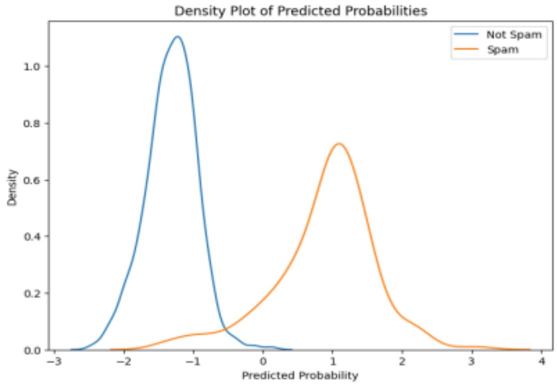

Chart -3: Density Plot Of Predicted Probabilities Chart

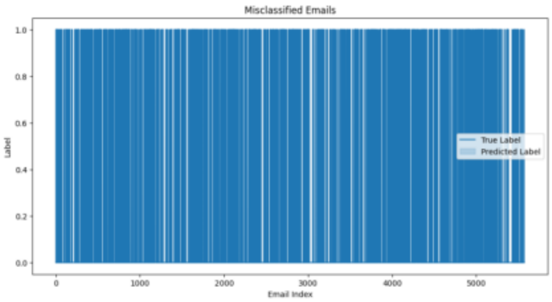

Chart -4: Lineplot Misclassified Emails Chart

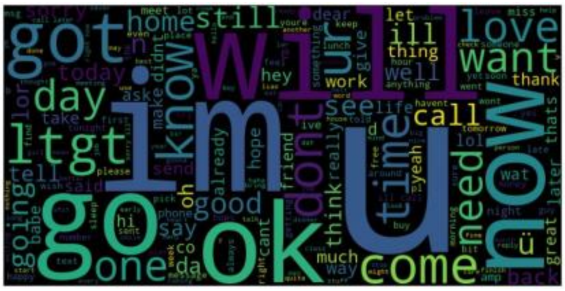

Chart -5: Word Cloud Non Spam

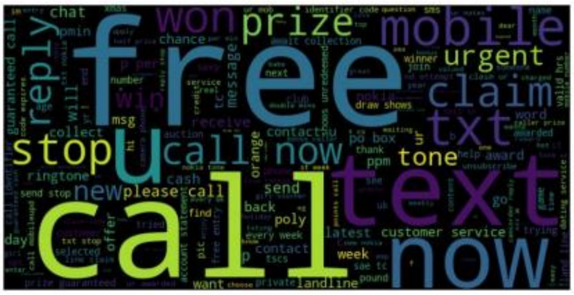

Chart -6: Word Cloud Spam

Classifiers	Mean Error	Values in (%)			
		MSE	MAE	RMSE	R-Square
Support Vector Classifier	1.0	01.52%	01.52%	12.34%	86.83%
Naïve Bayes	1.0	04.39%	04.39%	20.96%	62.04%
Decision Tree	1.0	03.85%	03.85%	19.63%	66.68%
K-Nearest Neighbour	1.0	07.62%	07.62%	27.61%	34.15%
Random Forest	1.0	02.86%	02.86%	16.94%	75.21%

Table -2 : EVALUATION TABLE

V. CONCLUSION

These abstract highlights the effectiveness of employing machine learning and the TF-IDF NLP technique for email spam detection. The proposed approach offers a valuable solution to combat the ever-growing threat of email spam, providing a robust and efficient mechanism for filtering out unwanted messages and protecting users from potential cyber security risks.

By creating an accurate and efficient email spam detection system, this project aims to contribute to the enhancement of email security, minimize the impact of spam emails on productivity, and protect users from potential cyber security threats.

VI. REFERENCES

[1]. Aaisha Makkar, Sahil (GE) Garg, Neeraj Kumar, M. Shamim Hossain, Ahmed Ghoneim, Mubarak Alrashoud,"An Efficient Spam Detection Technique for IoT Devices using Machine Learning" ,IEEE Transactions on Industrial Informatics (Volume: 17, Issue: 2, Feb. 2021)

[2]. Z. K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, andS. Shieh, "Iot security: ongoing challenges and research opportunities,"in 2014 IEEE 7th international conference on service-oriented computing and applications. IEEE, 2014, pp. 230–234.

[3]. A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smarthome," in 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops). IEEE, 2017, pp. 618–623.

[4]. E. Bertino and N. Islam, "Botnets and internet of things security," Computer, no. 2, pp. 76–79, 2017.

[5]. C. Zhang and R. Green, "Communication security in internet of thing: preventive measure and avoid ddos attack over iot network," Proceedings of the 18th Symposium on Communications & Networking. Society for Computer Simulation International, 2015, pp. 8–15.

[6]. W. Kim, O.-R. Jeong, C. Kim, and J. So, "The dark side of the internet: Attacks, costs and responses," Information systems, vol. 36, no. 3, pp.675–705, 2011.

[7]. H. Eun, H. Lee, and H. Oh, "Conditional privacy preserving security protocol for nfc applications," IEEE Transactions on Consumer Electronics, vol. 59, no. 1, pp. 153–160, 2013.

[8]. R. V. Kulkarni and G. K. Venayagamoorthy, "Neural network based secure media access control protocol for wireless sensor networks," in 2009 International Joint Conference on Neural Networks. IEEE, 2009, pp. 1680–1687.

[9]. M. A. Alsheikh, S. Lin, D. Niyato, and H.-P. Tan, "Machine learning in wireless sensor networks: Algorithms, strategies, and applications,"IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1996–2018, 2014.

[10]. A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2015.

[11]. F. A. Narudin, A. Feizollah, N. B. Anuar, and A. Gani, "Evaluation of machine learning classifiers for mobile malware detection," Soft Computing, vol. 20, no. 1, pp. 343–357, 2016.

[12]. N. Sutta, Z. Liu, and X. Zhang, "A study of machine learningalgorithms on email spam classification," in Proceedings of the 35th International Conference, ISC High Performance 2020, vol. 69, pp. 170–179,Frankfurt,Germa.

[13]. L. Xiao, Y. Li, X. Huang, and X. Du, "Cloud-based malware detection game for mobile devices with offloading," IEEE Transactions on Mobile Computing, vol. 16, no. 10, pp. 2742–2750, 2017.

[14]. J. W. Branch, C. Giannella, B. Szymanski, R. Wolff, and H. Kargupta, "In-network outlier detection in wireless sensor networks," Knowledge and information systems, vol. 34, no. 1, pp. 23–54, 2013.

[15]. I. Jolliffe, Principal component analysis. Springer, 2011.

Cite this article as :

K Usha Rani, Dosala Srinishma, Ancha Vidisha, "A Robust Approach for Effective Spam Detection Using Supervised Learning Techniques", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 10 Issue 4, pp. 49-54, July-August 2023.
Journal URL : https://ijsrset.com/IJSRSET23103158