International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)
ISSN: 2456-236X
Vol. 08 Special Issue 01 | 2023

A Framework Design for Email Spam Detection using Machine Learning

Prof.A. D. Bhople[1], Mayuri Prakash Warade[2], Priya Tulshiram Ghute[3],
Rekha Dnyaneshwar Gawande[4],Rohini Sanjay Narkhede[5],

[2]*Student, Computer Science and Engineering,Padm.Dr.VBKCOE,Malkapur Maharashtra, INDIA*
[3]*Student, Computer Science and Engineering,Padm.Dr.VBKCOE,Malkapur Maharashtra, INDIA*
[4]*Student, Computer Science and Engineering,Padm.Dr.VBKCOE,Malkapur Maharashtra, INDIA*
[5]*Student, Computer Science and Engineering Padm.Dr.VBKCOE,Malkapur Maharashtra, INDIA*

Abstract

Nowaday, emails are used in almost every field, from business to education. Emails have two subcategories, i.e., ham and spam. Email spam, also called junk emails or unwanted emails, is a type of email that can be used to harm any user by wasting his/her time, computing resources, and stealing valuable information. The ratio of spam emails is increasing rapidly day by day. Spam detection and filtration are significant and enormous problems for email and IoT service providers nowadays. Among all the techniques developed for detecting and preventing spam, filtering email is one of the most essential and prominent approaches. Several machine learning and deep learning techniques have been used for this purpose, i.e., Naïve Bayes, decision trees, neural networks, and random forest. This paper surveys the machine learning techniques used for spam filtering techniques used in email and IoT platforms by classifying them into suitable categories.

Keywords: ***Emails, spam, resources, detection, filtration***

1. INTRODUCTION

Email spam is a major problem for businesses and individuals alike, causing a significant amount of time and resources to be wasted on managing unwanted messages. In recent years, machine learning algorithms have been used to help combat email spam by automatically classifying emails as either spam or legitimate messages. In this paper, we will discuss the various approaches to email spam detection using machine learning.

1.1 Data Collection

The first step in building an email spam detection system is to collect data. A labeled dataset of emails is required, where each email is classified as spam or not spam. There are several publicly available datasets for this purpose, such as the Spam Assassin Public Corpus and the Enron email dataset.

1.2 Data Preprocessing

Once the dataset is collected, it needs to be preprocessed before being used for training a machine learning algorithm. This includes removing stop words, stemming, and tokenization. The preprocessing step is critical to improving the accuracy of the classification model.

1.3 Feature Extraction

The next step is to extract features from the preprocessed data. Common features used for email spam detection include the presence of certain keywords, the length of the email, and the frequency of certain words. Other features, such as the sender's email address and the IP address of the email server, can also be used.

1.4 Model Training

After feature extraction, a machine learning model can be trained on the preprocessed and feature-extracted data. Popular machine learning algorithms for email spam detection include Naive Bayes, Decision Trees, and Support Vector Machines. The performance of the model is typically measured using metrics such as precision, recall, and F1 score.

1.5 Evaluation and Testing

Once the model is trained, it needs to be evaluated and tested on a separate set of data. This helps to ensure that the model can generalize to new data and not just overfit to the training data. Various evaluation metrics can be used to assess the performance of the model, such as accuracy, precision, recall, and F1 score.

2. LITERATURE SURVEY

Email spam is nothing more than fake or unwanted bulk mails sent via any account or an automated system. Spam emails are increasing day by day, and it has become a common problem over the last decade. Email IDs receiving spam emails are typically collected through spambots (a computerized application that crawls email addresses across the Internet). The applications of machine learning have been playing a vital role in the detection of spam emails. It has various models and techniques that researchers are using to develop novel spam detection and filtering models [13]. Kaur and Verma [14] present a survey on email spam detection using a supervised approach with feature selection. They discuss the knowledge discovery process for spam detection systems. They also elaborate various techniques and tools proposed for spam detection. The choice of features based on N-Gram is also addressed in this survey. N-Gram [15, 16] is a predictive-based algorithm used to predict the probability of the next word occurrence after finding $N-1$ terms in a sentence or text corpus. N-Gram uses probability-based techniques for the next word prediction. They compare various machine learning (multilayer perceptron neural network support vector machine, Naïve Bayes) and nonmachine learning (Signatures, Blacklist and Whitelist, and mail header checking) approaches for email spam detection.

Blanzieri and Bryl [2, 19] describe a list of learning-based email spam filtering approaches. In this paper, they addressed the spam problems and provided a review of learning-based spam filtering. They explain various features of spam emails. In this study, effects of spam emails on different domains were discussed. Various economic and ethical issues of spam are also discussed in this study. The antispam approach that is common and learning-based

filtering is well developed. The commonly used filters are based on different classification techniques applied to various components of email messages. This study suggests that the Naïve Bayes classifier holds a particular position amongst multiple learning algorithms used for spam filtering. With splendid pace and simplicity, it gives high precision results.

Bhuiyan et al. [20] present a review of current email spam filtering approaches. They summarize multiple spam filtering approaches and sum up the accuracy on various parameters of different proposed systems by analyzing numerous processes. They discuss that all the existing methods are efficient for filtering spam emails. Some have successful results, and others are attempting to incorporate other ways to boost their accuracy performance. Although they are all successful, they still have some issues in spam filtering methods, which is the primary concern for researchers. They are trying to create a next-generation spam filtering mechanism to understand large numbers of multimedia data and filter spam emails. They conclude that most email spam filtering is done by utilizing Naïve Bayes and the SVM algorithm. To test the spam filtration models, these models can be trained on different datasets, such as "ECML" and UCI dataset [21].

Ferrag et al. [13] presented a review of deep learning algorithms of intrusion detection systems and spam detection datasets. They discussed various detection systems based on deep learning models and evaluated the effectiveness of those models. They examined 35 well-known cyber dataset by dividing them into seven categories. These categories include Internet traffic-based, network traffic-based, Interanet traffic-based, electrical network-based, virtual private network-based, andriod apps-based, IoT traffic-based, and Internet connected device-based datasets. They conclude that deep learning models can perform better than traditional machine learning and lexicon models for intrusion and spam detection.

3. SPAM MESSAGES

The email spam definition is ambiguous since everybody has their views on it. At present, email spam is getting the attention of everyone. Email spam ordinarily includes particular spontaneous messages sent in mass by individuals you do not know. The term spam is obtained from the Monty Python sketch [19], in which the Hormel canned meat item has numerous tedious emphases. While the term spam was purportedly first utilized in 1978 to allude to unwanted email, it increased rapidly in the mid-1990s, as we get to turn out to be progressively typical outside scholastic and research circles [20]. A notable model is the development expense trick in which a client receives an email with an offer that should bring about a prize. In the era of technology, the dodger/spammer shows a story where the unfortunate casualty needs forthright financial help so that the fraudster can gain a lot bigger total of cash, which they would then share. The fraudster will either earn a profit or avoid communication when the unfortunate victim completes the installment.

4. INTERNET OF THINGS AND IT ATTACKS

The Internet of things (IoT) means a system of interrelated, Internet-connected objects that collect and transfer data

over a wireless network without the intervention of humans. IoT enables the integration and implementation of real-world objects regardless of location. In such a scenario, privacy and security techniques are highly critical and challenging in network management and monitoring performance. To solve security problems, such as intrusions, phishing attacks, DoS attacks, spamming, and malware in IoT applications must protect privacy. Ios systems, including objects and networks, are vulnerable to network and physical attacks and privacy failures.

The various attacks of IoT systems are listed as follows.

(a) Self-Promotion Attack. In this type of attack, the compromised node tries to get importance over the other nodes of the IoT environment for the particular recommendation.

(b) Bad Mouthing Attack. In this attack, the compromised node forgave a wrong recommendation; it may execute the trust of the trusted node. It decreased the services of the trusted node.

(c) Ballot Stuffing Attack. In this challenge of the IoT environment, the compromised node enhances the other compromised nodes. It is a chance for the compromised node to provide the services. It is also known as the collision recommendation attack.

(d) Opportunistic Service Attack. In this type of attack, the compromised node collaborates with the other malicious nodes to build the bad mouthing and ballot stuffing attack.

(e) On-Off Attack. In this type of attack, the compromised node provides inadequate services, which means that the compromised node randomly performs a bad service. Node Tempering. The attacker changes the malicious node and gets specific information such as a security key.

(f) Malicious Node Attack. The attacker physically adds the malicious node among nodes.

(g) Man in the Middle Attack. The attacker secretly intercepts the communication between two nodes over the Internet in this type of attack. The attacker gets the main information by eavesdropping

(h) Sybil Attack. The compromised node steals the recognition of good nodes and acts as a suitable node.

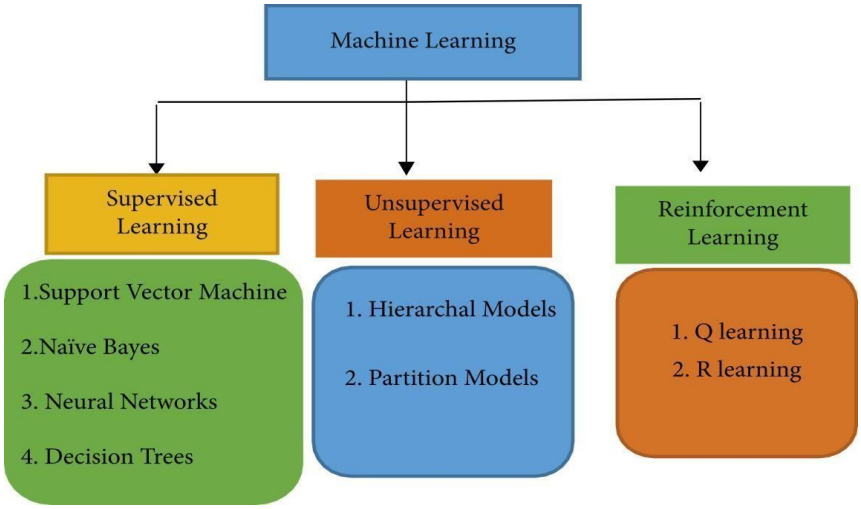

Fig.1 Types of Machine Learning

5. CONCLUSION

Email spam detection using machine learning is an effective way to combat the problem of unwanted emails. By collecting and preprocessing labeled datasets, extracting useful features, training machine learning models, and evaluating their performance, it is possible to build accurate and reliable email spam detection systems. While there is no one-size-fits-all approach to email spam detection, the methods discussed in this paper provide a good starting point for building such systems.

REFERENCES

[1] H. Faris, A. M. Al-Zoubi, A. A. Heidari et al., "An intelligent system for spam detection and identification of the most relevant features based on evolutionary random weight networks," Information Fusion, vol. 48, pp. 67–83, 2019.

[2] E. Blanzieri and A. Bryl, "A survey of learning-based techniques of email spam filtering," Artificial Intelligence Review, vol. 29, no. 1, pp. 63–92, 2008.

[3] A. Alghoul, S. Al Ajrami, G. Al Jarousha, G. Harb, and S. S. Abu-Naser, "Email classification using artificial neural network," International Journal for Academic Development, vol. 2, 2018.

[4] N. Udayakumar, S. Anandaselvi, and T. Subbulakshmi, "Dynamic malware analysis using machine learning algorithm," in Proceedings of the 2017 International Conference on Intelligent Sustainable Systems (ICISS), IEEE, Palladam, India, December 2017.

[5] S. O. Olatunji, "Extreme Learning machines and Support Vector Machines models for email spam detection," in Proceedings of the 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE), IEEE, Windsor, Canada, April 2017.

[6] J. Dean, "Large scale deep learning," in Proceedings of the Keynote GPU Technical Conference, San Jose, CA, USA, 2015.

[7] J. K. Kruschke and T. M. Liddell, "Bayesian data analysis for newcomers," Psychonomic Bulletin & Review, vol. 25, no. 1, pp. 155–177, 2018.

[8] K. S. Adewole, N. B. Anuar, A. Kamsin, K. D. Varathan, and S. A. Razak, "Malicious accounts: dark of the social networks," Journal of Network and Computer Applications, vol. 79, pp. 41–67, 2017.

[9] A. Barushka and P. Hájek, "Spam filtering using regularized neural networks with rectified linear units," in Proceedings of the Conference of the Italian Association for Artificial Intelligence, Springer, Berlin, Germany, November 2016.

[10] F. Jamil, H. K. Kahng, S. Kim, and D. H. Kim, "Towards secure fitness framework based on IoT-enabled blockchain network integrated with machine learning algorithms," Sensors, vol. 21, no. 5, p. 1640, 2021.

[11] M. H. Arif, J. Li, M. Iqbal, and K. Liu, "Sentiment analysis and spam detection in short informal text using learning classifier systems," Soft Computing, vol. 22, no. 21, pp. 7281–7291, 2018.

[12] X. Zheng, X. Zhang, Y. Yu, T. Kechadi, and C. Rong, "ELM-based spammer detection in social networks," The Journal of Supercomputing, vol. 72, no. 8, pp. 2991–3005, 2016.

[13] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: approaches, datasets, and comparative study," Journal of Information Security and Applications, vol. 50, Article ID 102419, 2020.

[14] N. Kumar and S. Sonowal, "Email spam detection using machine learning algorithms," in Proceedings of the 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), pp. 108–113, Coimbatore, India, 2020.

[15] I. Santos, Y. K. Penya, J. Devesa, and P. G. Bringas, "N-grams-based file signatures for malware detection," ICEIS, vol. 9, no. 2, pp. 317–320, 2009.

[16] S. Cresci, M. Petrocchi, A. Spognardi, and S. Tognazzi, "On the capability of evolved spambots to evade detection via genetic engineering," Online Social Networks and Media, vol. 9, pp. 1–16, 2019.

[17] H. Bhuiyan, A. Ashiquzzaman, T. Islam Juthi, S. Biswas, and J. Ara, "A survey of existing e-mail spam filtering methods considering machine learning techniques," Global Journal of Computer Science and Technology, vol. 18, 2018.

[18] A. Asuncion and D. Newman, "UCI machine learning repository," 2007, https://archive.ics.uci.edu/ml/index.php.

[19] L. N. Petersen, "The ageing body in monty Python live (mostly)," European Journal of Cultural Studies, vol. 21, no. 3, pp. 382–394, 2018.

[20] L. Zhuang, J. Dunagan, D. R. Simon, H. J. Wang, and J. D. Tygar, "Characterizing botnets from email spam records," LEET, vol. 8, pp. 1–9, 2008.

[21] W. N. Gansterer, A. G. K. Janecek, and R. Neumayer, "Spam filtering based on latent semantic indexing," in Survey of Text Mining II, pp. 165–183, Springer, New York, NY, USA, 2008.