Journal of Theoretical and Applied Information Technology
15th July 2023. Vol.101. No 13
© 2023 Little Lion Scientific

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

EMAIL SPAM FILTERING TECHNIQUE: CHALLENGES AND SOLUTIONS

SHARIFAH MD YASIN[1], IQBAL HADI AZMI [2]

[1, 2] Faculty Computer Science and Information Technology,

Universiti Putra Malaysia, Malaysia

E-mail: [1]ifah@upm.edu.my, [2]gs61356@student.upm.edu.my

ABSTRACT

For many years, practically all industries, from business to education, have used electronic mail for either personal or corporate communication. Spam, often known as unsolicited email, can be used to harm any user and computing resource by stealing important data. Email conversations frequently involve sensitive and private information. Emails are therefore useful to scammers since they able to use these facts for bad purposes. The primary goal of the attacker is obtaining personal data through deception email recipients into opening malicious links or downloading attachments. Cyberthreats have grown significantly during the past few years. The most common cybercrime that makes use of spam emails as a tool is phishing. Email phishing has caused significant identity and financial losses. Spam detection and filtering is a critical and important problem. There are numerous strategies that can be utilized to counter email spam. No technique has, however, been shown to be particularly successful. Some approaches, such as applying machine learning, have a very high potential for minimizing the issues with email phishing. Reviewing filtering mechanisms, particularly those used in email, is crucial for understanding how they work and for spotting potential problems. Based on predetermined criteria, a number of papers on spam email were acquired from various digital sources. The most relevant papers that had just been released were chosen. Many researchers are interested in the methods used to filter spam and emails. One of the most significant and well-known methods for identifying and preventing spam is email filtering. These approaches have been contrasted. In order to identify phishing emails, this paper describes a machine learning (ML) approach. It talks about issues and anticipated future developments. In order to categorize phishing emails at various levels of crime, numerous ML models that have been suggested throughout the years are compared and reviewed.

Keywords: *Phishing, Email, Spam, Machine Learning, Analysis of algorithms*

1. INTRODUCTION

The mechanism being utilised to distribute information has become highly quick and simple to use as technology progresses. Users can choose from a variety of platforms to communicate and share information with one another. The email system is among the most significant and widely used forms of communication. Sending and receiving information is crucial to our day-to-day activities. Emails can be used for a variety of purposes, including notification, business, personal, advertising, and other uses. The cost effectiveness and speed of email communication can be attributed to the system's popularity. Spam emails, regrettably, pose a threat to the email system. Spam emails can raise the threat to email users, and email itself has security flaws that can come from the information that recipients receive [1].

Any inappropriate and undesired communication or email sent to many recipients by the attacker is referred to as spam [2]. As a result, the email platform's security concerns must be addressed. More than half of the user's email is received as spam, according to the author in [3]. To effectively use email without having to worry about risks like losing personal information, a spam filtering system should be developed. The undesired emails sent by some individuals, often known as spammers, are considered spam emails for spam detection [4]. Regrettably, the expansion of online services and the Internet has coincided with an increase in cyberattacks, with phishing being one of the most prevalent and successful attacks. The emergence of the cyber world brought with it new threats in the form of malicious hacker-performed cyberattacks.

Phishing-related breaches required the third-longest length of time to identify and prevent, lasting 295 days on average, according to IBM's 2022 Data Breach Report [5]. Due of uncontrolled access to personal information, phishing is still a significant issue today. In order to effectively counter phishing, it must be recognised and addressed, adopting intrusion detection approach [6]. Phishing is the practise of transmitting messages that are fake but come from what appears to be a reliable source. The goal is to trick the recipient into revealing confidential details or putting malicious software similar to spyware on the victim's computer. Phishing is the practise of attempting to obtain personal information while posing as a trustworthy source. The effectiveness of phishing emails, according to [7], is related to the manipulation of human emotions, which would make the victim worried and create an urgent situation by warning that failing to answer swiftly would result in a substantial loss of money and data.

Email communication is a crucial part of everyday business activities and is frequently used by attackers as a point of entry into the targeted organisation. There are many issues with hacking, attacks on management weaknesses in cloud servers and distributed denial of service attacks are both progressively developing [8]. Attackers have the capacity to send the recipient potentially damaging content via email messages, including links to dangerous websites or malware attachments. The loss or disclosure of crucial data is one of the many negative effects that these attacks typically have on the organisation. A false email or other kind of contact used to attract a target is how phishing starts. The message is written to appear to have come from a reliable source. If the target falls victim, they could be convinced to reveal personal information, typically on a fake website. On rare occasions, malware may also be downloaded onto the victim's computer.

Sometimes, attackers are willing to steal credit card numbers and personal information in order to profit. Phishing emails may also be sent in other cases in an attempt to get employee login credentials or other information that will be utilised in more serious attacks on a select group of people or a specific company [9]. 86% of businesses reported having at least one worker who has accepted a phishing link, according to CISCO's analysis of cyber security threat trends for 2021. Throughout the year, the frequency of phishing attacks varies. Phishing attacks increased by 52% in December, according to Cisco research, showing that the holidays are when they peak. The weakest link in security, users are the target of these attacks. The widespread use of social engineering methods demonstrates that system weaknesses are less frequently the focus of attackers [10].

Phishing is one of the most prevalent and successful attacks. Even though numerous detection have been suggested, the large amount of phishing emails necessitates further work [6]. The author in [11] suggests that additional work on detection algorithms is required due to the dynamic nature of phishing emails. Spam filtering is essentially email sorting, but its main objective is the elimination of unwanted emails. Several well-known email spam detection techniques are employed to address the spam issues. Spam emails have been filtered using a variety of approaches and methods.

However, as the current approach is inadequate, a more successful one is needed to stop hacking. By examining the spam sample database utilising spam keywords and content text analytics, the author in [12] proposed an algorithm that categorises various sorts of spam threads in 2020. By using this method, spam threads that continually appear will be eliminated, and better solutions for stopping spammers' ethical hacking will be provided. Due of uncontrolled access to personal information, phishing is still a significant issue today. In order to effectively counter phishing, it must be recognised and addressed, adopting intrusion detection approach.

Spam email is currently a major issue on the internet. Spam stops the user from fully and effectively utilising their time, storage, and network resources. The massive amount of spam that circulates around computer networks has a negative impact on email servers' memory, communication bandwidth, CPU power, and user time [13]. Additionally, users find receiving spam emails to be quite annoying. Many users have also suffered financial loss as a result of online fraud and other dishonest activities by spammers who send emails purporting to be from reputable businesses in an effort to trick people into disclosing sensitive personal information like passwords, Bank Verification Numbers (BVN), and credit card numbers. Healthcare and dating spam were the two most prevalent categories of spam emails. Simple Mail Transfer Protocol (SMTP) servers must process a large number of unsolicited emails, which results in an inefficient use of resources [14].

The rest of this paper is organized as follows: Section 2 presents a related work. Section 3 describes phishing email detection using machine learning. Then, Section 4 presents result and discussion. Finally, Section 5 presents the conclusion of this paper.

2. RELATED WORKS

Comparatively recent research on email spam detection has been done largely in the previous five years. The growth of spam emails is one of the biggest problems affecting our globally linked communication networks since email is accessible to anybody with an internet connection. Unauthorized spam mail may be on the rise as a result of the rise in hacker activities in the modern world over the past few years. These cyberattacks frequently cause a tremendous deal of harm to the organisation, including the loss or disclosure of critical data [15]. As spam incidence keeps rising, there is a greater demand for antispam filters that are more dependable and efficient. All currently work spam filtering algorithms must be weighed for advantages and disadvantages, and any flaws must be fixed or at the very least minimised [14]. There are various methods for detecting email spam, and these problems must be overcome. Spam emails are rapidly expanding in popularity in the fields of politics, education, messages, stock market guidance, and marketing [16].

Spam email volume is likely to rise as more people use the internet. Innovation in technology is being abused for immoral and illegal practises like phishing and scamming. Detecting online spammers has grown to be a significant social issue because of the threat they bring to internet security [17]. Spam detection offers a number of rules and methods to enable secure communications between individuals and organisations [18]. Spam filtering is essentially email sorting, but its main objective is the elimination of unwanted emails. Several well-known email spam detection techniques are employed to address the spam issues. Although many detectors have been proposed, more research is necessary due to the enormous number of phishing emails [6]. The secret to phishing emails' effectiveness is their ability to play on recipients' fears and sense of urgency by threatening major financial and data losses if they do not take action right away. A classifier model for phishing emails that makes use of deep learning methods and a graph convolutional network (GCN) was researched in [6] to improve the precision of phishing detection. The classifier was found to be effective at identifying phishing emails. The spam filtering model and method outlined, according to [19], need to be improved because they have not yet shown to be 100% accurate predictors. A pre-trained transformer model called Bidirectional Encoder Representations from Transformers can be adjusted to fulfill the function of distinguishing between phishing and legitimate emails. For spam identification, the use of learning-based classifiers [20] is popular these days. It is assumed that spam emails have a certain set of features that distinguish them apart from regular emails in the detection process for learning-based categorization [21].

Several variables affect the difficulties of spam identification in learning-based models. These components include overhead processing, concept drift, linguistic problems, text delay, and spam subjectivity. The fundamental concepts, efforts, outcomes, and study patterns of spam filtering are described by [14]. The most recent study examines the ways in which the leading ISPs' spam filters, including those for Gmail, Yahoo, and Outlook, analyse spam emails using machine learning contexts. Both the fundamental approach to detect phishing and the several researchers' attempts to prevent spam with machine learning methods have drawn criticism. The study assesses the benefits and drawbacks of the existing machine learning approaches and highlights fresh issues with the establishment of spam filters. In order to effectively counter the threat, the study recommended extensive education as risk control techniques for spam e-mail.

Numerous studies support the effectiveness of incorporating textual cues to improve phishing classifier performance [22]. From the websites' source code, URL, and client side only, the authors derive nineteen features. The majority of the data is gathered from the websites Phishtank, Openphish, and Alexa, it has 1918 legitimate websites and 2141 phishing websites among its 4059 websites in the training dataset. The authors used simple techniques in order to produce a labelled dataset, the feature vector was created, with a unique feature vector being created for each instance of a webpage. The dataset has been examined using 10-fold cross-validation. With SVM, the study achieved 99.09% accuracy, and with neural networks, 98.05%.

There are several existing algorithms being researched to identify the optimum solution, and various sorts of data sets could be used. The method includes both previously completed work and novel techniques that might be applied if the findings are satisfactory. Once an email has been classified as spam, it should be divided into many categories to reveal its content and level of severity. The procedure for conducting experiments to determine the optimal spamming approach is shown in Figure 1. It serves as the fundamental framework for the methods used to categorise spam and non-spam emails.

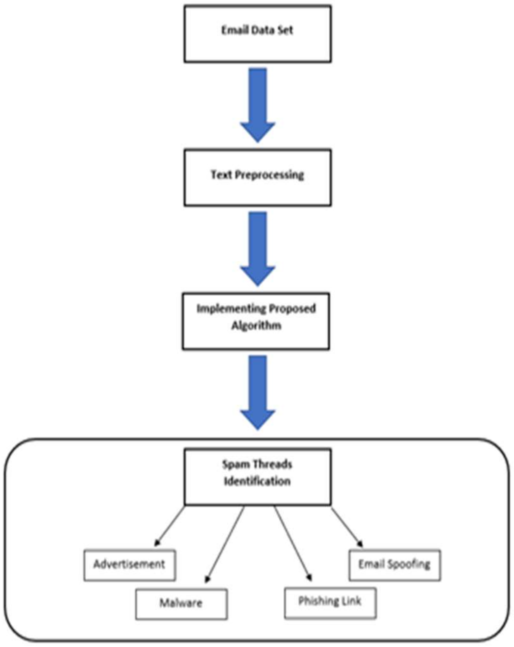

Figure 1. Stages of spam technique implementation

The following sections provide information on the machine learning algorithms, procedures, and spam filtering strategies.

3. PHISHING E-MAIL DETECTION USING MACHINE LEARNING

Despite the fact that many research articles have been published using different machine learning algorithms to identify and manage spam emails, there are still certain research gaps. Spam email is one of the most significant and interesting study topics for closing the gaps [23]. As a result, in order to improve the credibility and usefulness of email communication for consumers, several studies on the identification of spam have previously been carried out using a range of approaches.

Machine learning, which enables computer systems to automatically learn and enhance their performance without explicit programming, is one of the most essential and effective uses of artificial intelligence (AI). The three most popular machine learning techniques are Naive Bayes, SVM, and NN.

The main goal of machine learning technique is to design systems that can automatically retrieve and utilise data for training. The initial step in the curriculum is to acquire labelled data, also referred to as a training dataset. Learning labelled data, often named as a training dataset, is the first step in the learning process [24]. The authors of [3] analysed email text using a natural language processing method in attempt to identify spam. The authors claim that machine learning approaches enable the most accurate classification of spam. It was suggested to use broad descriptive features extracted from all email components using machine learning approaches to improve the identification of fake emails [15]. Machine learning makes it easier to deal with huge amounts of information. Even while it typically provides faster and more accurate findings to detect dangerous content, it can be more expensive and time-consuming to train its models for a high degree of performance.

Combining AI and cognitive computing with machine learning can enhance the power of handling enormous amounts of data [25]. Machine learning is illustrated in several forms in Figure 2.

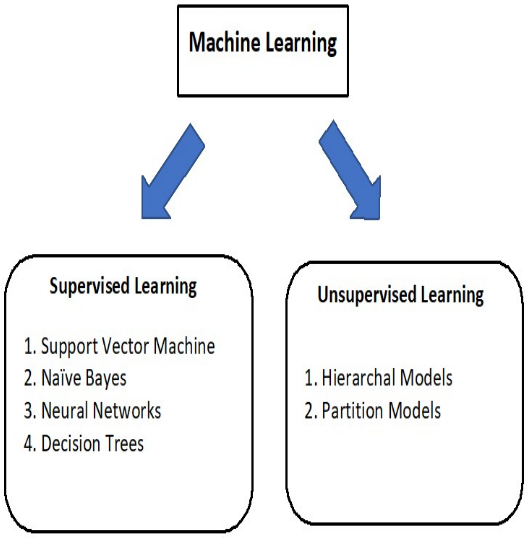

Figure 2: Types of machine learning

In supervised learning, labelled data are used to train models that can forecast new data. This type of training can be used to solve a variety of problems, such as the popularity of advertisements, the categorization of spam, face recognition, and object classification. Unsupervised learning creates clusters of the data based on its attributes using unlabeled data. This kind of learning can be applied to a number of issues, including grouping user logs, recognising purchasing patterns, and recommender systems. The following are some of the most popular supervised learning approaches.

3.1 Support Vector Machine (SVM)

A Support Vector Machine (SVM) is a type of machine learning algorithm that is commonly used for classification and regression analysis. SVMs have been found to be effective in a variety of applications, including image classification, text classification, and bioinformatics. The approach for statistical spam filters using SVM, Naive Bayes, KNN and regression trees was provided by the author [26]. These supervised machine learning methods were utilised by the authors in [27], and the precision, recall, and accuracy of the findings were evaluated. The researchers used the Sina Weibo social network and the machine learning model SVM to identify spammers. This study's dataset consisted of 16 million messages that were gathered from various individuals. As a feature vector set, they used 18 features.

Spammers and authorised users were the two categories into which the networks' users were separated. 20% of the data was used for testing, while the remaining 80% was used for the model's training. The author employed a 1:2 ratio of spammers to non-spammers in the training dataset to increase accuracy. The proposed model provides a 99.5% accuracy level with this ratio. Extreme learning machine and support vector machine techniques were employed in [28] to create a spam filtering programme. The spam detection model developed using a standard dataset and SVM had an accuracy of 94.06% and an advanced machine learning model had a 93.04% accuracy level. The results show that SVM was able to enhance performance by 1.1%. In those circumstances, the proposed spam detector ought to be chosen instead of SVM spam detection, where detection speed is crucial, such as in real-time systems. Despite having a greater accuracy level in the research, the author claims that SVM requires more training time.

3.2 Naive Bayes Classifier (NB)

A Naive Bayes classifier is a probabilistic machine learning algorithm used for classification tasks. It is based on the Bayes' theorem and assumes that the features of a given data point are independent of each other. The algorithm calculates the probability of a data point belonging to a particular class based on the probability of each feature being present in that class. It selects the class with the highest probability as the prediction. Using a variety of performance measures, the authors in [29] provided a piece on spam detection strategies based on machine learning techniques. The training of the suggested models utilised a significant number of input features. Based on the input attributes, each model calculates a spam score. The authors claim that their suggested technique can identify spam more accurately than spam detection tools currently in use. It has to be improved how well the Naive Bayes Spam Filter classifies emails as garbage or not and detects text changes, the author of [30] suggested using a novel approach. To improve the accuracy of Naive Bayes, a Python approach that combines keyword, semantic, and machine learning techniques was applied.

Similar to this, the authors of [31] discussed using ML algorithms to identify email spam. In this article, they examine ML techniques and how to apply them to datasets. From a variety of ML algorithms, the most precise and accurate method for email spam detection is found. The authors came to the conclusion that the class conditional independence of the Naive Bayes algorithm, which results in the machine misclassifying some inputs, limits its ability to generate the optimal results.

3.3 Artificial Neural Networks

An Artificial Neural Network (ANN), also known as a neural network, is a type of machine learning model that is inspired by the structure and function of the human brain. ANNs are composed of interconnected nodes, called neurons, that are organized in layers. The algorithms have been essential for identifying scam emails and a variety of tasks, including classification, regression, and clustering. They can learn to recognize patterns and relationships in data through a process called training. There are many types of ANNs, including convolutional neural networks, and recurrent neural networks. Each type is optimized for a specific type of data or task.

Researchers are employing its numerous models and methodologies to develop cutting-edge spam detection and filtering algorithms. A type of filtering called standard spam filtering implements a set of rules and uses those rules as a classifier. The content filters use artificial intelligence algorithms to recognise spam [32]. As a result, it would be feasible to better identify phishing emails using machine learning techniques. Various latent feature elements are also possible to be retrieved from the perspective of various information networks. An identification of spammers using a Deep Graph neural network is shown from the perspective of a diverse internet as a second approach to the same problem [17]. Similar to this, the author of [33] recommended using artificial neural networks, whose accuracy is close to 98.8% to enhance spam identification.

The operational characteristics of biological neural networks, often known as "neural networks," serve as the foundation for the computational model known as an artificial neural network (ANN) [34]. In a neural network, numerous sets of neurons are connected, and data is processed using a computational technique link. Most of the time, during the learning phase, neural network is an intelligent system that alters its architecture in response to information flowing in via the network, whether it is internal or external. The neural network's fundamental structure is depicted as in Figure 3.

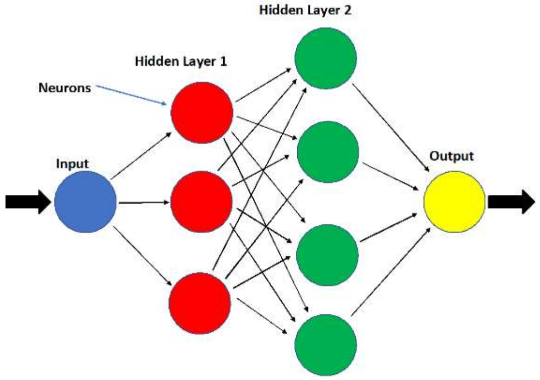

Figure 3: Neural network fundamentals

A few of the machine learning-based proposed methods for email spam identification and prevention have been developed summarised in Table 1.

Table 1: Phishing email detection techniques.

No	Algorithm	Accuracy	Advantage	Limitation
[6]	natural language processing with graph convolutional networks	98.20 %	a single, massive graph created from email data	The concept depends on the text classification
[16]	Bidirectional encoder representations	98.67 %	deep learning algorithms is used	based on a small input data, 300 sequence length
[14]	Deep Graph neural network based model	90.74 %	Real world datasets were used	time for training with more features not evaluated
[29]	Recurrent convolutional neural network	95.02 %	using a character level, features extracted from URL	may misclassify some of the phishing sites, training time long
[13]	Recurrent Convolutional Neural Networks	99.85 %	multilevel vectors and attention mechanism	cannot detecting phishing emails with email body only
[15]	Convolutional neural network	95.97 %	DL and ML techniques for pre processing	accuracy of DL models better, but computation time of ML models better

The most accurate algorithm based on the table is the recurrent convolutional neural network. This is because the activities of the units can evolve as time pass by. This feature will enhance the ability of the model to integrate the context information which plays a crucial role for object recognition. The accuracy result from each paper is different depending on the parameters being used. The best algorithm chosen to be used should be able to achieve the goals and the weaknesses should be at an acceptable level. The optimization technique from the paper [14] could be considered poor which resulted it in having lower accuracy. There has been no method proven to be invincible which results in different algorithm being used for different purpose.

4. DISCUSSION

From Table 1, we identify different algorithm being used which resulted in [15] having the best result which is 99.85% and the lowest result of accuracy is 90.74% from [14]. The dataset used includes many different types such as publicly available and real world dataset. Some of the algorithm requires some condition to apply while other type of algorithm is flexible and easy to apply. In [17], the algorithm being used can only support a small input of data which is 300 sequence length. Based on Table 1, the majority of the datasets used to develop, test, and adopt different models seems to have been produced artificially. The difficulty of categorising every supervised model data set, coupled with the shortage of analytical examples. As a result, the predictions of the classifiers are not entirely reliable due to the usage of artificial datasets during model training.

Considering how many machine learning models are presently used for identification or screening spam email, these reviews of spam are not indicative of real-world situations. By examining and evaluating various methodologies, this survey research describes the methods and models for spam filtering that are based on machine learning that are now in use. For conclusion, we present the summary of the accuracy of the various proposed approaches and an overview of various spam filtering strategies. It was discovered that all spam filtering methods work effectively. While some are attempting to utilize alternative strategies to improve accuracy, some have achieved amazing achievements. Even if they are all useful, some are still lacking from the spam filtering system, which is the main reason why researchers are concerned.

This study provides a more thorough investigation into the most recent technologies for reducing email spamming and which produce the most effective results. This review might potentially suggest a new approach that could be adopted and have better results while posing less risks. From Table 1, the goal of the researcher is to develop cutting-edge spam filtering technologies that can utilise multimedia content and efficiently screen spam emails. In order to improve accuracy and efficiency, hybrid algorithms will probably replace the supervised and unsupervised learning algorithms that are now used for spam detection. In future work can enhance such as feature extraction. Spam and legitimate email can be better clustered using clustering approaches for spam filtering relevant feedback by dynamically updating it. Future email spam detection methods could possibly make use of other concepts and approaches in addition to machine learning. In the future, experts may work together to manually annotate datasets, leading to the creation of efficient, standardised, and highly dimensional spam databases. Using approaches that are flexible, low energy-consuming, and capable of real-time processing, with faster processing and more precise classification, spam filters can be made. The availability of common labelled datasets for researchers to train classification models, as well as the addition of extra features to the dataset to improve the accuracy and reliability of spam detection models, such as the IP address and location of the attacker, must also be the research priorities in the future. The email's header, topic, and message content were taken into account by the researchers when classifying emails as spam.

Despite the fact that these features are insufficient to produce totally accurate results, manual feature selection must be incorporated. Almost all studies published their findings based on accuracy, precision, and recall, despite the fact that computational complexity of algorithms for machine learning models should be thought of as an evaluative metric. It is possible to increase error detection, self-learning, and speed of response by utilising comprehensive features and an accurate preprocessing stage. Since the majority of present filters are unable to alter their feature space, learning models with dynamic feature space updating must be implemented for better spam classification. For increased accuracy and dependable outcomes, a spam detection and filtration system need to be secure.

Another important research field that might be investigated is multilingual spam recognition which is necessary for better spam detection methods. In addition, it is also possible to investigate a linguistic feature combination for the spam detection method. There is currently no reliable way to handle problems with the security of spam filters. This kind of attacks may be random, exploratory, or targeted. Spam detection systems face a major difficulty as a result of the Internet's expanding volume of data and multiple additional features. Although there have been several studies on a related subject, this study presents the most recent machine learning research that may assist in reducing the issue of email spam.

5. CONCLUSION

Over the recent years, a considerable research community has become interested in spam identification and filtration. This topic has received a lot of investigation since it frequently has a costly and major impact in many circumstances. The survey examines several machine learning techniques and strategies that various scholars have proposed for email spam detection and filtering. The study comes to the conclusion that supervised machine learning techniques provide the foundation of the majority the suggested methods for detecting spam emails.

The objective of the paper is to present a concise overview of the various machine learning models and techniques currently being used for email spam detection. It provides a thorough analysis of the operation of real phishing email identification from several perspectives. However this study might have given more attention to machine learning, and there might be some other approach that works better without using machine learning.

To recognise phishing emails, a variety of machine learning algorithms have been utilised, but these techniques fall short in their ability to recognise ongoing phishing scams, which requires intensive manual feature engineering. This phishing email detection has a number of unresolved problems, and the results indicate that more work is needed. Phishing emails have been growing at broad variety rates over the past few years, and despite continual updating and revision, the defenses employed to address this evolving threat have not been successful. More sophisticated phishing detection technology is required to handle this email threat.

There are many types of algorithm that provides different percentage of accuracy and efficiency but each has their own advantages and disadvantages. The dataset being used is also different for each algorithm that is used by the research. Each algorithm has different capabilities and flexibilities which could also determine the time for processing. This study has helped to ensure that the research can choose the appropriate methods and combine them if necessary to obtain the best findings by examining a variety of methods. Additionally, it offers information on current techniques, particularly those that integrate machine learning.

REFERENCES:

[1] H. Faris, A.M. Al-Zoubi, A.Heidari, I. Aljarah, M.Mafarja, M.A. Hassonah and H. Fujita. "An intelligent system for spam detection and identification of the most relevant features based on evolutionary Random Weight Networks". *Inf. Fusion, 48*, 2019. pp. 67-83.

[2] A.Alghoul, S.AlAjrami, G.AlJarousha, G. Harb and S.S. Abu-Naser, "Email Classification Using Artificial Neural Network" *International Journal of Engineering, 2*, 2018. pp. 8-14.

[3] Y. Kontsewaya, E. Antonov and A. Artamonov, A. "Evaluating the effectiveness of machine learning methods for spam detection" *Procedia Computer Science,* 190, 2021. pp. 479-486.

[4] J.K. Kruschke and T.M. Liddell, "Bayesian data analysis for newcomers". *Psychonomic Bulletin & Review,* 25, 2018, pp. 155-177.

[5] Data Breach Report, https://www.ibm.com/downloads/cas/3R8N1DZJ retrieved 15 December 2022.

[6] F. Aburub and W. Hadi, "A new association classification based method for detecting phishing websites". *Journal of Theoretical and Applied Information Technology*, 99(1), 2021, pp.147-158.

[7] A.Alhogail and A. Alsabih, "Applying machine learning and natural language processing to detect phishing email". *Computers & Security*, 110, 2021. 102414.

[8] C.Jang, O. Lee, C. Mun and H. Ha. An Analysis of Phishing Cases using Text Mining. *Journal of Theoretical and Applied Information Technology*, 100(22), 2022.

[9] What is phishing, https://www.cisco.com/c/en/us/products/security/email-security, retrieved 15 December 2022.

[10] Cyber security threat trends- phishing, crypto top the list. https://umbrella.cisco.com/info/ 2021-cyber-security-threat-trends-phishing-crypto-top-the-list, retrieved 15 December 2022.

[11] B.B. Gupta, N.A.G. Arachchilage and K.E. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions". *Telecommun Syst* 67, 2018, pp. 247–267

[12] U. Murugavel and R. Santhi, "Detection of spam and threads identification in E-mail spam corpus using content based text analytics method". *Materials Today: Proceedings*, 33, 2020, pp. 3319-3323.

[13] D.M. Fonseca, O.H. Fazzion, E. Cunha, I. Las-Casas, P.D. Guedes, W. Meira, M. Chaves,

"Measuring characterizing, and avoiding spam traffic costs", *IEEE Int. Comp.,* 99, 2016.

[14] E.G. Dada, J. S. Bassi, H. Chiroma, S.M. Abdulhamid, A.O. Adetunmbi and O.E. Ajibuwa, "Machine learning for email spam filtering: review, approaches and open research problems". *Heliyon*, 5, 6, 2019, pp. 1-23.

[15] A. Cohen, N. Nissim and Y. Elovici, "Novel set of general descriptive features for enhanced detection of malicious emails using machine learning methods". *Expert Systems with Applications,* 110, 2018, pp. 143-169.

[16] Y. Fang, C. Zhang, C. Huang, L. Liu and Y. Yang, "Phishing E-mail Detection Using Improved RCNN Model With Multilevel Vectors and Attention Mechanism" *in IEEE Access,* vol. 7, 2019, pp. 56329-56340.

[17] Z. Guo, L, Tang, T. Guo, K. Yu, M. Alazab and A. Shalaginov, "Deep graph neural network-based spammer detection under the perspective of heterogeneous cyberspace". *Future generation computer systems,* 117, 2021, pp. 205-218.

[18] S. Bagui, D. Nandi and R.J. White, "Machine Learning and Deep Learning for Phishing Email Classification using One-Hot Encoding", *Journal of Computer Science*. 17(7), 2021, pp. 610-623.

[19] I. AbdulNabi and Q.Yaseen, "Spam email detection using deep learning techniques". *Procedia Computer Science*, 184, 2021. pp. 853-858.

[20] M. Vijayalakshmi, S. Mercy Shalinie, M. H. Yang and R. Meenakshi, "Web phishing detection techniques: a survey on the state-of-the-art, taxonomy and future directions", *IET Networks*, vol. 9(5), 2020, pp. 235–246.

[21] S.Salloum, T.Gaber, S.Vadera and K. Shaalan, "Phishing E-mail Detection Using Natural Language Processing Techniques: A Literature Survey", *Procedia Computer Science*, vol. 189, 2021, pp. 19-28.

[22] A. K. Jain and B. B. Gupta, "Towards detection of phishing websites on client-side using machine learning based approach," *Telecommunication Systems*, vol. 68, 2018, pp. 687-700, doi: 10.1007/s11235-017-0414-0

[23] S. Pitchaimani, V.P. Kodaganallur and C. Newell, "Systems and methods for controlling email access," *Google Patents*, 2020.

[24] E. Alpaydin, "Introduction to Machine Learning", *MIT Press, Cambridge*, UK, 2020.

[25] A. D. Garcez, M. Gori, L. C. Lamb, L. Serafini, M. Spranger, and S. N. Tran, "Neural-symbolic computing: an effective methodology for principled integration of machine learning and reasoning," *Journal of Applied Logic*, vol. 6, 2019.

[26] W. Peng, L. Huang, J. Jia, and E. Ingram, "Enhancing the naive bayes spam filter through intelligent text modification detection," 17th *IEEE International Conference on Trust, Security and Privacy In Computing And Communications/12th IEEE International Conference on Big Data Science And Engineering (TrustCom/BigDataSE*), IEEE, August 2018.

[27] K. Lei, Y. Liu, S. Zhong, Y. Liu, K. Xu, Y. Shen and M. Yang, "Understanding user behavior in Sina Weibo online social network: a community approach," *IEEE Access*, 6, 2018. pp. 13302–13316.

[28] S.O. Olatunji, "Improved email spam detection model based on support vector machines," *Neural Computing & Applications*, vol. 31, no. 3, 2019, pp. 691–699.

[29] 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, 2018, pp. 7281–7291.

[30] N. Mageshkumar, A. Vijayaraj, N. Arunpriya and A. Sangeetha. "Efficient spam filtering through intelligent text modification detection using machine learning", *Materials Today*, 64, 1, 2022, pp. 848-858.

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

[32] A. Aljofey, Q. Jiang, Q. Qu, M. Huang and J. P. Niyigena, "An Effective Phishing Detection Model Based on Character Level Convolutional Neural Network from URL", *Electronics*, 9, 9, 2020, pp. 1514.

[33] D. Mallampati, N.P. Hegde, "A machine learning based email spam classification framework model: related challenges and issues", *Int. J. Innovative Technol. Exploring Eng*., 9.4, 2020, pp. 3137-3144.

[34] N. Sutta, Z. Liu, and X. Zhang, "A study of machine learning algorithms on email spam classification," *the 35th International Conference, ISC High Performance 2020,* 69, 2020, pp. 170–179.