Phishing Email Detection Using Machine Learning Techniques

Hussain Alattas[1], Fay Aljohar[2], Hawra Aljunibi[3], Muneera Alweheibi[4], Rawan Alrashdi[5], Ghadeer Al azman[6], Abdulrahman Alharby[7] and Naya Nagy[8]

University of Imam Abdulrahman bin Faisal, College of Computer Science, and Information Technology, KSA

Abstract

Phishing is a social engineering technique that mainly aims to steal personal or confidential data and may harm the target individual or organization in many ways. In phishing, fraudsters hide their identity as legitimate people, banks, or institutions, whether governmental or private. And since e-mail communication is the most used method in transmitting confidential or official messages, fraudsters normally target the email users to send their deceptive messages in order to extract data. However, this paper presents an overview of previously conducted studies with respect to detecting phishing email messages using machine learning. The paper's objective is to analyze and assess the procedures of previously proposed models, datasets, and their results within the specified scope.

Keywords:

Phishing Attacks, Machine Learning, Phishing Emails, Social Engineering, Email Security.

1. Introduction

Phishing emails represent a threat in the world of the Internet, as email is the main place to send messages, whether personally or officially, as many individuals depend on it and review it daily. The interaction of one individual in an organization with a phishing message may lead to the destruction of the entire organization, this is what we mean by a threat phishing message. In this paper, we discuss some of the previous research on detecting phishing attacks in email and some models and suggested features in detecting these attacks. We also present a comparative study of classic machine learning techniques such as Random Forest, Random Forest, Naive Bayes, Decision Tree, and Support Vector Machine (SVM). This paper is sectioned by a problem statement, background, review of literature that has three sub-sections supervised machine learning techniques, non-supervised, and others; moreover, it illustrates a comparison table between models in the aspect of approaches, limitations, algorithms, response time, and accuracy.

2. Problem Statement

A phishing attack is generally accomplished by sending email messages that appear to come from a trusted source and require the user to enter financial, personal, or confidential data. The problem is when the user interacts with the email and sends the requested response, either by replying to the email by sending confidential data, visiting a website, or clicking on a link. Attackers are always coming up with new and inventive ways to dupe people into thinking their activities are related to a legitimate website or email. The user interacts without thinking when the situation seems to be dangerous, fearful, urgent, etc. Most end users usually make the decision based on how they look and feel.

3. Background

In the early 1990s, a huge number of users with false credit card details created an algorithm for stealing user information, they registered themselves on America Online (AOL) site without any validation and started using system resources. When AOL eliminated the random credit card generators in 1995, the Warez group shifted to other techniques, including communicating with individuals via AOL Messenger while pretending to be AOL employees and requesting their personal information. In 1996, American On line's Usenet group posted the first mention of the term "phishing" in response [1]. Phishing occurs when cybercriminals send malicious emails to trick a victim into falling for a scam. The goal is usually to persuade users to divulge sensitive information such as financial data or system credentials. The advantages of phishing for cybercriminals include its simplicity, low cost, and effectiveness. Attackers can easily gain access to valuable information with very little effort and for a low price. Due to this, we are going to discuss a variety of machine learning models to detect such phishing e-mails and then block them [1]. Machine learning is a method of analyzing data that automates the process of constructing analytical models. This branch of artificial intelligence relies on the idea that computers can identify patterns, learn from data, and make decisions without the need for any human interference [2].

4. Review of literature

As phishing emails constitute the primary gateway to phishing websites, several papers were examined that discuss phishing email detection and classification

Manuscript received April 5, 2022
Manuscript revised April 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.4.79

techniques. A major approach for phishing email detection and classification is to employ machine learning techniques.

4.1 Machine Learning and Phishing Emails Detection

Machine learning is a critical ally in fighting phishing emails. Mostly, it investigates the content, metadata, context, and regular user behavior to analyze and detect phishing. Machine-learning includes several types such as supervised machine learning which utilizes label data to train models, and unsupervised machine learning which utilizes patterns from unlabeled data to train them. Though, unsupervised machine learning may give less accurate results compared to supervised machine learning [3]. Examples of previous work regarding these machine learning techniques are going to be discussed in the subsequent sections.

4.1.1 Supervised Machine Learning Techniques

As described in [4], A. Shaheen et al. proposed a model based on supervised machine learning algorithms to classify phished and ham mail. In supervised learning algorithms, a training set is used to classify test sets. The dataset consists of 1605 emails, 1191 are ham and 414 are phished. Ham emails are derived from a publicly available dataset, while phished emails are derived from multiple sources. After preprocessing and converting the dataset, features were extracted and used to feed the classifiers. The features are extracted from the dataset using the Python programming language and the Nerve Learning Toolkit. The dataset consists of extracted features is segmented and fed into five classifiers: Logistic, Random Forest, SVM, Voted Perceptron, and Naive Bayes. Results showed that the classification of emails through SVM and Random Forest classifiers was highly accurate, achieving the highest accuracy of 99.8%.

Akash Junnarkar et al. [5] built a comprehensive system for spam classification using semantics-based text classification and URL-based filtering. They establish a spam classification system that followed a two-step methodology to ensure that all mail received was either spam or not. The process begins with text classification and is followed by URL analysis and filtering to determine whether any links present in the email are malicious. Five machine learning algorithms were considered for text classification: K-Nearest Neighbours, Naive Bayes, Decision Tree, Random Forest, and SVM. The highest accuracy is obtained with Naive Bayes and SVM, hitting a 97.83 % accuracy rate for SVM and 95.48 % for Naive Bayes. As Naive Bayes and S had the highest accuracy, they were implemented in the final model to identify trigger words within the text. Lists of spam trigger words and blacklisted URLs were compiled using several datasets. The model was hosted as an API that was called by JavaScript code in Google Apps script to process emails in real-time.

In [6], Jameel et al. proposed a phishing detection model that uses a feed-forward neural network. The model was created based on the characteristics of phishing emails. Thus, a set of 18 features were extracted from the tested email, these email features appear in the header and the HTML body of the email. In a subsequent step, a multilayer feedforward neural network is used to classify the tested email into phishing or ham email. A total of 9100 phishing and ham emails have been used to test this model; 4550 of these emails are phishing emails were collected from publicly available phishing Corpus (www.monkey.org), while 4550 of these samples are ham emails were collected from the Spam Assassin project's ham corpora. According to the testing results, the identification rate of this model was excellent (98.7%).

A method based on neural networks was proposed by George et al. [7]. The team used two datasets consisting of 4500 emails phish and ham. To identify ham and phish emails, they applied various algorithms, including Feedforward Neural Network (FNN) with back propagation, and fist order statistical measures. As a result, the false-negative rate and the false positive rate are exceptionally low. With 12 features, 99.95% of the results were classified correctly.

Kumar et al. [8] investigated the detection of phishing emails lacking links and URLs. In their proposed work, they have used NLP and WordNet. Using 600 phishing emails and 400 legitimate emails, they have compiled a list of features including the absence of recipients' names, asking for money, or mentioning money, a sense of urgency, and a sense of urgency that lures victims to respond. They had based their work on Stanford Core NLP's application program interface to identify all the words found in phishing emails.

Harikrishnan et al. proposed [9] (Term Frequency Inverse Document Frequency) TFID+ (Singular Value Decomposition) SVD and TFIDF+ (Nonnegative Matrix Factorization) NMF to evaluate if it is in fact phishing email or not. The model starts by using email datasets with and without headers passed to data pre-processing. Then, to convert words to a numeric representation it uses TFIDF. After that, it uses SVD and NMF to extract features. Lastly, to decide whether it is legitimate or not, classical Machine Learning (ML) techniques are utilized. The accuracy of the result for this model was low due to the highly imbalanced dataset.

Senturkurk et al. [10] proposed a model that begins with data set training by concentrating on the email's body and ignoring the attachments and header. After the data sets are ready, it starts the feature selection. Then passed it to Waikato Environment for Knowledge Analysis (WEKA) tool after converting it to the proper format. Later, a sub-list is initiated below this new decision node and a sub-decision tree is built. After that, a different algorithm used: Naïve Bayes and decision tree. Finally, the result shows it will appear high accuracy rate when a supplied test is selected and performing datasets for all operations is in a real-time environment.

The proposed approach by Hamid et al. [11] is called the Hybrid Feature Selection (HFS). HFS applies to 6923 datasets from both Nazario and SpamAssassin datasets. In addition, it analyzes the sender behavior to resolve a feature matrix utilizing seven email relevant features to determine whether an email is phishing or not. Further, in order for HFS to classify the email, it uses an algorithm named Bayes Net algorithm for email classifications.

As shown by Adewumi and Akinyelu [12] the Firefly Algorithm (FFA) is combined with the (SVM) for machine learning classification to build a hybrid classifier called FFA_SVM. For the purpose of evaluating the FFA_SVM algorithm, a database was constructed of 4000 phishing and ham emails along with their features. FFA_SVM has outperformed the standard SVM.

Alayham et al. [13] design and develop a tool that detects the source code of a phishing site associated with a Gmail account using a decision tree algorithm and generates a report of phishing sites attached to a victim's email as the percentages of phishing emails stored in the user's mailbox. Also, the application can send notifications to the user regarding a phishing site that was detected in the incoming message. The Agile Unified Process (AUP) methodology was used to implement the tool.

Husak and J. Cegan [14] Develop an automated tool to deal with PhiGARo phishing incidents that identify individuals who respond to phishing attack attempts. The network traffic of the honeypot is monitored, and any phishing emails detected are sent to the PhiGARo tool. The PhiGARo framework is divided into two parts, the Phishing Incident Handling section and the Phishing Response and Detection section. Initially, the phishing incident is reported by the user who recognizes the phishing message in their mailbox. PhiGARo is implemented by Incident Handler manually, then interpreting the results, blocking the phishing email or URL, and finally notifying the victims.

Egozi and Verma [15] created a phishing email detection tool with 26 features. Features include word count, stop words, repeating punctuation, and unique words. 17 machine languages were studied and categorized under weighted and unweighted, based on the results, the weighted linear SVM algorithm represented the best model.

Unnithan et al. [16] proposed a model based on a variety of mathematical algorithms to measure if an email is a legitimate email or not. Consists of two dataset emails with headers and without headers. This sample is sent to count-based representation Term Frequency Inverse Document Frequency (TFIDF) and then combined with domain-level features to convert the input to an understandable input for machine learning algorithms. The last step in the model to decide whether it is a legitimate or phishing email is passed to several machine learning such as logistic regression, Naive Bayes, SVM.

4.1.2 Unsupervised Machine Learning Techniques

Fuertes et al. [17] is described how to develop a Scrum-based algorithm implementation of automatic learning, feature selection, and neural networks, with the goal of attack detecting and mitigating from inside the email server. The samples were divided into three different time periods and tested on a different dataset that was previously merged. Feature Selection, Neural Networks, Agile Scrum methodology, and Matlab process tool are used during the implementation of the proposed algorithm. Because the developed methods complement each other during detection, the acquired results from the concept tests are highly promising. The findings of the three data sets were evaluated, and the average accuracy was 93.9%, and to validate the results obtained the source of information from the Phish Tank blacklist was used.

Andrade et al. [18] create a Python software that uses a machine-learning algorithm to learn how to recognize bad URLs, then provides relevant analysis and information about the bad URLs. The program also includes an examination of the analysis of anomalous behavior linked to phishing web attacks, as well as how machine learning techniques may be used to counter the problem. This analysis is carried out using tainted datasets provided by Kaggle Phishing Dataset and Python tools to develop machine learning to detect phishing attacks by analyzing URLs to determine whether they are good or bad based on specific characteristics of URLs, with the goal of providing information in real-time so that proactive decisions can be made to reduce the impact of the attack. When information is added to machine learning algorithms and the algorithm is performed, the accuracy and error are likely to improve.

Unnithan et al. [19] proposed a model based on a variety of mathematical algorithms to measure if an email is a legitimate email or not. Consists of two dataset emails with headers and without headers. This sample is sent to count-based representation TF-IDF and then combined with domain-level features to convert the input to an understandable input for machine learning algorithms. The last step in the model to decide whether it is a legitimate or phishing email is passed to several machine learning such as logistic regression, Naive Bayes, Support Vector Machine. The accuracy of this model after testing

4.1.3 Other Machine Learning Techniques

The proposed phishing detection model in [20] by Viktorov, uses a dataset of phishing and non-phishing emails from different websites. The model starts with preprocessing the collected data to extract features from each email. Second, passed to feature selection which splits into two scenarios. Those scenarios are automated and manually. In the manually use clustering, which is like classification, but it is unsupervised. third, it is passed to the classification selection phase. fourth to multi-classifier, that uses several algorithms to build it such as Logistic regression, Decision Tree and Sequential minimal optimization. The results showed that clustering will increase the accuracy rate.

Rastenis et al. [21] discuss the Multi-Language Spam/Phishing Classification solution that classifies an unwanted email to either spam or phishing emails classes through using the email body content and a dataset that is constructed by three other known data sets: Nazario, SpamAssassin, and VilniusTech. Additionally, it can classify the email even if it is written in Russian and Lithuanian languages rather than just English through integrating with existing classifying emails solutions and automated translation.

Fang et al. proposed [22] an approach named THEMIS (Greek word) that uses unbalanced dataset and divides the email into two parts: the email's header and body. Then, it splits it more into two levels: the char-level, and word-level for both header and body. Also, it calculates the likelihood if an email is phishing by comparing the probability with a classification value called a threshold, if the probability is greater than this value then it is a phishing email.

Li et al. have presented [23] the overall function of the Long Short-Term Memory (LSTM) Network method for big email data. LSTM cannot use an open-source dataset; thus, a filter must be conducted manually first of the nature of the phishing emails the enterprise receives. After a filter has been established, both supervised KNN and unsupervised K Means are used to conduct labeling automation to construct a set of samples used for phishing email detection.

5 Comparison

This section represents a comparison between given machine learning techniques discussed in the literature to detect phishing emails. The comparison is based on which algorithm(s) or model(s) had been used, accuracy, Ture Positive Rate (TPR), False Positive Rate (FPR), datasets used, number of features, response time, and drawbacks.

5.1 Supervised Machine Learning Techniques Comparison Table.

Author	*Algorithm(s) used*	*Accuracy*	*TPR*	*FPR*	*Datasets used*	*No. of Features*	*Response time*	*Drawbacks*
Supervised Machine Learning Techniques								
[4]	Random Forest	99.87%	99.9%	0.2%	N. A	9	N. A	Data used may not reflect real life scenarios
[5]	SVM	97.83 %	53.0%	3.0%	Enron Data set and spam.csv Kaggle data	N. A	N. A	There is no real-time learning of email classifiers in the provided data sets
[6]	FNN	98.72%	98%	1.2%	N. A	18	0.00000067 seconds	Increased numbers of neurons will increase training and testing time

[7]	FNN	99.95%	100%	0.09%	N. A	12	0.00000118 seconds	N. A
[8]	NLP	99.4%	N. A	N. A	N. A	N. A	N. A	Unable to extract text from email attachment
[11]	Bayes Net	94%	0.97%	0.13%	Nazrario & SpamAssassin	7	N. A	Graphical form in phishing emails cannot be detected
[12]	SVM	99.94%	N. A	0.01%	Dataset consists of 4000 emails	16	0.16 seconds	N. A
[9]	Decision Tree	96.5%	92%-97%	8%-26%	PhishingCorpus	7	8.54 seconds	Dataset is highly imbalanced
	Random Forest	97.1%					Slow	
	KNN	97.6%					4.3 Seconds	
	Naive Base	94.7%					0.01 seconds	
	AdaBoost	97.7%					N. A	
	SVM	98.7%					0.16 seconds	
	Logistic Regression	96.8%					12.11 seconds	
[10]	Naïve bayes	89%	N. A	N. A	MIME	13	0.01 seconds	Datasets must be in real-time environment to success
	Decision Tree						8.54 seconds	
[13]	Decision Tree	95.05%	N. A	N. A	Used 3 available dataset	8	8.54 seconds	N. A
[14]	IPFIX	N. A	N. A	Low	N. A	N. A	3 to 19 per day	Must support the trustworthiness of honeytokens and honeypots
[15]	SVM	90%	83.0%	96.0%	IWSPA	28	0.16 seconds	Takes few hours to run
[16]	Naïve Bayes	79.5%	N. A	N. A	Enron and Avocado	N. A	0.01 seconds	Cannot extract feature from headers
	SVM	88.4%	3593/4583	489/4583			0.16 seconds	
	Logistic Regression	80.1%	N. A	N. A			2.11 seconds	

Table 1: Supervised Machine Learning Techniques Comparison

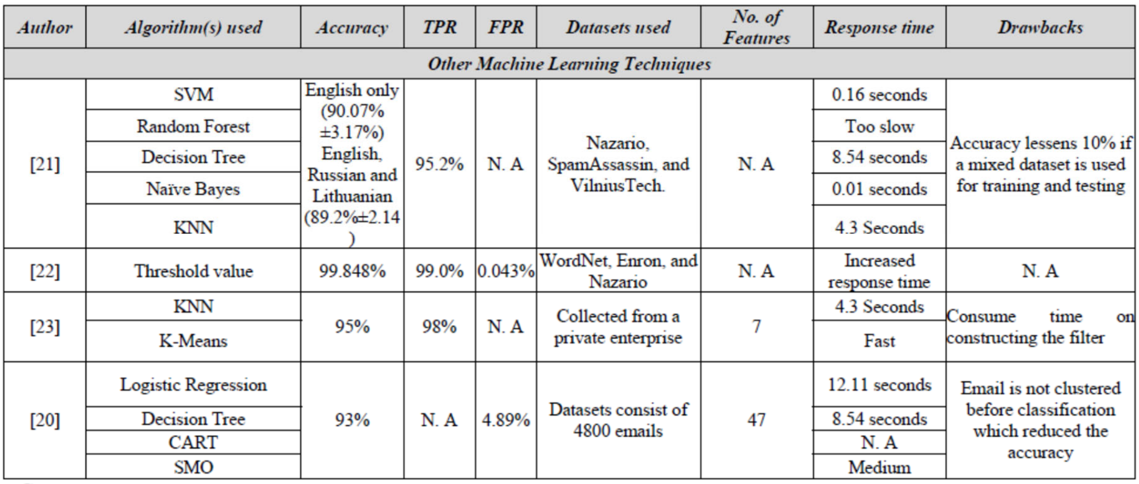
5.2 Unsupervised Machine Learning Techniques Table.

Author	*Algorithm(s) used*	*Accuracy*	*TPR*	*FPR*	*Datasets used*	*No. of Features*	*Response time*	*Drawbacks*
Unsupervised Machine Learning Techniques								
[17]	Agile Scrum	93.9%	N. A	2.7%	Debian Phish Tank	7	N. A	N. A
[18]	Logistic	90%	N. A	N. A	Kaggle	N. A	12.11 seconds	N. A
[19]	SVM	95%	3807/3572	7/217	N. A	5	N. A	cannot extract features from headers
	Naïve Bayes	94%						
	Logistic Regression	96%						

Table 2: Unsupervised Machine Learning Techniques Comparison.

5.3 Other Machine Learning Techniques Table.

Table 3: Other Machine Learning Technique



Author	*Algorithm(s) used*	*Accuracy*	*TPR*	*FPR*	*Datasets used*	*No. of Features*	*Response time*	*Drawbacks*
Other Machine Learning Techniques								
[21]	SVM	English only (90.07% ±3.17%) English, Russian and Lithuanian (89.2%±2.14)	95.2%	N. A	Nazario, SpamAssassin, and VilniusTech.	N. A	0.16 seconds	Accuracy lessens 10% if a mixed dataset is used for training and testing
	Random Forest						Too slow	
	Decision Tree						8.54 seconds	
	Naïve Bayes						0.01 seconds	
	KNN						4.3 Seconds	
[22]	Threshold value	99.848%	99.0%	0.043%	WordNet, Enron, and Nazario	N. A	Increased response time	N. A
[23]	KNN	95%	98%	N. A	Collected from a private enterprise	7	4.3 Seconds	Consume time on constructing the filter
	K-Means						Fast	
[20]	Logistic Regression	93%	N. A	4.89%	Datasets consist of 4800 emails	47	12.11 seconds	Email is not clustered before classification which reduced the accuracy
	Decision Tree						8.54 seconds	
	CART						N. A	
	SMO						Medium	

s Comparison.

5.4 Analysis

According to the comparisons in Tables 1, 2, and 3, four main models had been considered as remarkable models among others based on different parameters for email classification. These models are SVM, NLP, Random Forest and Naive Bayes models. Despite the fact that they had gained popularity in many previous works regarding email classification techniques SVM, NLP, Random Forest, and Naive Bayes algorithms have very high accuracy, TPR, and FPR compared to other algorithms with fast response times. On the other hand, two datasets had also gained popularity in the phishing detection field to extract informative email features for classification, these are Spam Assassin and Nazario corpuses. However, our literature study had shown that there are many effective algorithms of email classification, yet attackers are becoming more and more sophisticated with powerful techniques. Thus, each time ones want to decide which algorithms or learner are best to distinguish if an email is a phishing or non-phishing email is now becoming a difficult challenge.

6 Conclusion

Over the past few years, the problem of phishing emails has become more common. Phishing is a type of attack. The intention of phishing is to obtain personal information, such as passwords, credit card numbers, or other account information, by using emails. Phishing emails closely resemble legitimate ones, making it hard for a layperson to distinguish them. Machine learning techniques currently play a major role in phishing email detection and classification. Several models and approaches are available for phishing email detection. Each approach has its own unique advantages and capabilities, as well as limitations. Hence, this literature review has summarized and compared several methods and approaches for protecting against phishing email attacks.

References

[1] P. Verma, A. Goyal, and Y. Gigras, “Email phishing: text classification using natural language processing,” Comput. Sci. Inf. Technol., vol. 1, no. 1, pp. 1–12, 2020.

[2] E. Bisong, “What is machine learning?” in ” in Building Machine Learning and Deep Learning Models on Google Cloud Platform, Berkeley, CA: Apress, 2019, pp. 169–170.

[3] Gatefy, “How artificial intelligence and machine learning fight phishing,” Gatefy, 22-Mar-2021. [Online]. Available: https://gatefy.com/blog/how-ai-and-ml-fight-phishing/. [Accessed: 13-Mar-2022].

[4] S. Rawal, A. Shaheen, and S. Malik, “Phishing Detection in E-mails using Machine Learning,” Int. J. Appl. Inf. Syst., vol. 12, no. 7, pp. 21–24, 2017.

[5] A. Junnarkar, S. Adhikari, J. Fagania, P. Chimurkar, and D. Karia, “E-mail spam classification via machine learning and natural language processing,” in 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), 2021.

[6] N. Ghazi, M. Jameel and L. E. George, “Detection of phishing emails using feed forward neural network,” Int. J. Comput. Appl., vol. 77, no. 7, pp. 10–15, 2013.

[7] A. A. Abdullah, L. E. George, and I. J. Mohammed, “Research Article Email Phishing Detection System Using Neural Network,” Research Journal of Information Technology, vol. 6, no. 3, pp. 39–43, 2015.

[8] Aggarwal, Shivam, Vishal Kumar and Sithu D. Sudarsan. “Identification and Detection of Phishing Emails Using Natural Language Processing Techniques.” SIN (2014).

[9] B, Harikrishnan & Ravi, Vinayakumar & Kp, Soman. (2018), "A Machine Learning Approach Towards Phishing Email Detection," CEN-Security@IWSPA 2018.

[10] Ş. Şentürk, E. Yerli and İ. Soğukpınar, "Email phishing detection and prevention by using data mining techniques," 2017 International Conference on Computer Science and Engineering (UBMK), 2017, pp. 707-712, doi: 10.1109/UBMK.2017.8093510.

[11] I. R. A Hamid, J. Abawajy, and T.-H. Kim, “Using feature selection and classification scheme for automating phishing email detection,” Stud. Inform. Contr., vol. 22, no. 1, pp. 61–70, 2013.

[12] O. A. Adewumi and A. A. Akinyelu, “A hybrid firefly and support vector machine classifier for phishing email detection,” Kybernetes, vol. 45, no. 6, pp. 977–994, 2016.

[13] R. Alayham, C. Ren, J. Arshad and A. Muhammad, "Email Anti-Phishing Detection Application", Management & Science University, 2019.

[14] M. Husak and J. Cegan, "PhiGARo: Automatic Phishing Detection and Incident Response Framework", Masaryk University, Brno, Czech Republic, 2021.

[15] G. Egozi and R. Verma, "Phishing Email Detection Using Robust NLP Techniques", Department of Computer Science University of Houston, Houston TX, USA, 2021.

[16] Unnithan, Nidhin A., et al. "Machine learning based phishing e-mail detection." Security-CEN@ Amrita (2018): 65-69.

[17] L. Zapata, D. Ona, G. Rodriguez, and W. Fuetres, "Phishing Attacks: Detecting and Preventing Infected E-mails Using Machine Learning Methods", Universidad de las Fuerzas Armadas ESPE, Sangolqui, Ecuador, 2019.

[18] I. Ortiz-Garc, R. Andrade and M. Cazares, "Detection of Phishing Attacks with Machine Learning Techniques in Cognitive Security Architecture", Politecnica Salesiana,Quito, 2021.

[19] Unnithan, Nidhin A., et al. "Machine learning based phishing e-mail detection." Security-CEN@ Amrita (2018): 65-69.

[20] Viktorov, Oleg. "Detecting phishing emails using machine learning techniques." PhD diss., Middle East University, 2017.

[21] J. Rastenis, S. Ramanauskaitė, I. Suzdalev, K. Tunaitytė, J. Janulevičius, and A. Čenys, “Multilanguage spam/phishing classification by email body text: Toward automated security incident investigation,” Electronics (Basel), vol. 10, no. 6, p. 668, 2021

[22] Y. Fang, C. Zhang, C. Huang, L. Liu, and Y. Yang, “Phishing email detection using improved RCNN model with multilevel vectors and attention mechanism,” IEEE Access, vol. 7, pp. 56329– 56340, 2019.

[23] Q. Li, M. Cheng, J. Wang, and B. Sun, “LSTM based phishing detection for big email data,” IEEE Trans. Big Data, pp. 1–1, 2020.

Authors Biography

Muneera Alweheibi, Rawan Alrasheddi, Fay Aljohar, and Hawra Aljunibi: are currently pursuing their Bachelors degree in Cyber Security and Digital Forensics at the department of Networks and Communications, College of Computer Science and Information Technology (CCSIT), Imam Abdulrahman Bin Faisal University, Dammam. Mainly, their research interests include email security, Artificial Intelligence and Machine Learning.

Hussain Alattas is currently working in the department of Networks and Communications Department, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University (IAU), as a lecturer. Hussain has completed his BS degree in Computer Science from IAU and MS degree in Cybersecurity and Artificial Intelligence from The University of Sheffield.

Ghadeer Alazman is currently working in the department of Networks and Communications Department, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University (IAU), as a teaching assistant. Ghadeer has completed his BS degree in the science of Cyber Security and Digital Forensics from IAU.