IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 18, 2022, accepted June 10, 2022, date of publication June 14, 2022, date of current version June 24, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3183083

A Systematic Literature Review on Phishing Email Detection Using Natural Language Processing Techniques

SAID SALLOUM[1], TAREK GABER[1,2], SUNIL VADERA[1], AND KHALED SHAALAN[3]

[1]School of Science, Engineering and Environment, University of Salford, Salford M5 4WT, U.K.
[2]Faculty of Computers and Informatics, Suez Canal University, Ismailia 41522, Egypt
[3]Faculty of Engineering and IT, The British University in Dubai, Dubai, United Arab Emirates

Corresponding author: Said Salloum (s.a.s.salloum@edu.salford.ac.uk)

ABSTRACT Every year, phishing results in losses of billions of dollars and is a major threat to the Internet economy. Phishing attacks are now most often carried out by email. To better comprehend the existing research trend of phishing email detection, several review studies have been performed. However, it is important to assess this issue from different perspectives. None of the surveys have ever comprehensively studied the use of Natural Language Processing (NLP) techniques for detection of phishing except one that shed light on the use of NLP techniques for classification and training purposes, while exploring a few alternatives. To bridge the gap, this study aims to systematically review and synthesise research on the use of NLP for detecting phishing emails. Based on specific predefined criteria, a total of 100 research articles published between 2006 and 2022 were identified and analysed. We study the key research areas in phishing email detection using NLP, machine learning algorithms used in phishing detection email, text features in phishing emails, datasets and resources that have been used in phishing emails, and the evaluation criteria. The findings include that the main research area in phishing detection studies is feature extraction and selection, followed by methods for classifying and optimizing the detection of phishing emails. Amongst the range of classification algorithms, support vector machines (SVMs) are heavily utilised for detecting phishing emails. The most frequently used NLP techniques are found to be TF-IDF and word embeddings. Furthermore, the most commonly used datasets for benchmarking phishing email detection methods is the Nazario phishing corpus. Also, Python is the most commonly used one for phishing email detection. It is expected that the findings of this paper can be helpful for the scientific community, especially in the field of NLP application in cybersecurity problems. This survey also is unique in the sense that it relates works to their openly available tools and resources. The analysis of the presented works revealed that not much work had been performed on Arabic language phishing emails using NLP techniques. Therefore, many open issues are associated with Arabic phishing email detection.

INDEX TERMS Phishing email detection, systematic literature review, natural language processing, machine learning.

I. INTRODUCTION

Concerns about security issues have become more intense with developments in internet technologies and the consequent revolution in online user interaction. The evolving security issues pose threats to the internet user and may lead to monetary and identity loss for the user. Phishing is a kind of social engineering threat that exploits the ignorance of uninformed internet users to obtain sensitive information from them in a deceiving manner. Phishers or attackers present themselves as genuine internet users. Phishers make attempts to get illegitimate access to a victim's accounts to obtain sensitive or personal data and identity. Therefore, phishing and the associated criminal acts must be prevented. According to the Anti-Phishing Working Group (APWG), the number of phishing emails grew from 44,008 in the first

The associate editor coordinating the review of this manuscript and approving it for publication was Chao Tong.

quarter of 2020 to 128,926 by the third quarter [1]. As per the latest reports generated by APWG, the early months of 2020 showed about 68,000 to 94,000 attacks on a monthly basis; however, currently there has been a tremendous rise in phishing attacks. In July, 2021, APWG recorded the highest ever monthly phishing attack count of 260,642 phishing emails [2].

Since the outbreak of coronavirus in 2019 (COVID-19), the issue of phishing attacks has become a subject of major interest. During the period from September 2020 till now, a number of studies have been initiated to investigate phishing attacks with respect to COVID-19 [3]–[5]. Phishers usually hunt their potential victims by using text and information related to the COVID-19 pandemic [1]. The data revealed a significant rise in phishing attacks and their consequent impact specifically during the COVID-19 pandemic.

The most common phishing attack vectors include communication channels like emails and other messaging apps. Amongst all the methods, phishers prefer attacks by e-mails given they are difficult to detect [6]; hence, this study focusses on phishing attacks via email communication [7], [8].

Although various researchers have been exploring the world of phishing for over 10 years to gain insight into this major issue, there has been no significant development and no improvement in the prevalence of phishing attacks. This may be due to one or more of the following reasons: phishing is more complex than human perception, the practical techniques applied by researchers may have overlooked the main problem parameters, phishing attacks misuse the unawareness of the human users which may not be tackled merely by technical methods and may require human interventions like human training and awareness [9]–[13]. Although there have been several reviews that aim to identify the trends in detecting phishing attacks, it is important to assess the issue from different perspectives [9]–[13]. None of the surveys have ever comprehensively studied the use of NLP techniques for detection of phishing except one [14]. The work in [14] aimed to survey the work published using NLP and ML for detecting phishing emails but has not systematically reviewed all published papers in the last 10 years.

This paper offers a comprehensive literature review of studies that aim to utilise natural language processing (NLP) and machine learning (ML) methods for detecting phishing emails. The survey aims to answer the following research questions:

1. What are the key research areas in phishing email detection using NLP?
2. Which ML algorithms are used most for developing models for detection of phishing emails?
3. What are the main optimisation techniques used in detecting phishing emails?
4. What are the feature extraction methods in phishing email detection using NLP studies?
5. Which NLP techniques are used most in phishing email detection studies?
6. Which datasets and resources have been used in phishing email detection using NLP studies?
7. What are the evaluation criteria of the machine/deep learning techniques that have been used in phishing email detection using NLP studies?
8. What are the tools used in phishing detection email using NLP studies?
9. Which parts of the email are the most widely used in phishing detection email using NLP studies?
10. What are the trends across time in phishing email detection using NLP studies?
11. What proportion of phishing email detection studies are on mixed language models?

The rest of the paper is organised as follows. Section two presents a summary of the relevant studies that were carried out concerning phishing detection. The third section describes the classification of various phishing detection methods along with the suitable text review. The fourth section presents a systematic review of the selected papers according to the phishing email finding methods with different views, as follows: (1) phishing email detection datasets; (2) phishing email detection features; (3) phishing email detection techniques; and (4) evaluation metrics. Section five demonstrates the discussion. Finally, section six presents the conclusion, and future work.

II. LITERATURE REVIEW

As mentioned above, there have a number of surveys about phishing detection. This section therefore begins by summarizing and referencing the existing surveys. The reviewed studies have been classified on the basis of 1- uniform resource locators (URLs), 2- websites, 3- emails, and 4- general surveys.

A survey was conducted recently on studies pertaining to phishing URL detection [15]. This survey specifically focused on features of various ML and phishing URL detection techniques like batch, online, representation. Moreover, some studies pertaining to phishing URL detection were reviewed by [16]–[18], while literature on the domain of phishing URL detection and relevant issues were explained by [19], [20]. A novel multi-dimensional method for classifying phishing attacks was put forward in the survey by Mohammad *et al.* [20] who classified activities into five categories, namely: ML, text mining, human users, profile matching, and others. The researchers also suggested classifying the last category into search engines, ontology, client-server authentication, and honeypot countermeasures.

The topic of detection of phishing websites has been surveyed by five different research teams [9], [21]–[24]. Dou *et al*. [9] considered different perspectives and analysed the phishing detection techniques being used currently. They provided the phishing statistics and the contextual knowledge related to the phishing ecosystem. Subsequently, they performed a systematic review of various automatic phishing detection techniques and: (i) classified these phishing

detection techniques; (ii) explained the training and datasets used for the evaluation of phishing detection techniques; (iii) gave an account of the features involved in the detection schemes along with the fundamental detection algorithms and (iv) describe the evaluation metrics used in these techniques. Mohammad *et al.* [21] surveyed various papers on phishing website detection with respect to blacklist/whitelist, decision support tools, intelligent heuristics, immediate protection, and community rating services like Web of Trust. Some other detection techniques including search-based, visual-similarity, DNS-based, and proactive phishing URL-based techniques were analysed by Varshney *et al.* [22] who gave a detailed account of the benefits and drawbacks associated with the concerned detection approaches and techniques. They also presented a summary and indicated data sizes for a few of these papers. Tang and Mahmoud [23] have also performed a survey of phishing website detection techniques. They initially analysed the phishing life cycle, followed by the overview of basic anti-phishing methods that helped detect phishing links, offering a detailed account of ML-based solutions. They explored data collection, feature extraction, modelling, and evaluation performance, and compared different phishing website detection solutions. Qabajeh *et al.* [24] explored phishing techniques and highlighted the use of content-based techniques for detection of phishing. They presented a brief account of phishing, evaluated automatic phishing detection techniques, and their role and effectiveness in combating phishing website attacks.

The surveys highlighting multiple dimensions of phishing detection fall under the category of general surveys [10], [25]–[28]. Khonji *et al*. [25] conducted a literature review to examine studies relevant to anti-phishing techniques (such as user training, email sifting and website detection besides others). They extensively studied the classification of phishing e-mails, phishing detection methods and evaluation metrics. The phishing detection techniques analysed involved training strategies to reduce the human weakness factor by enhancing human awareness, along with a few software-based detection techniques. Das *et al*. [10] also considered the security challenges associated with phishing and performed user research for examining phishing and spear phishing detection techniques. Additionally, they conducted a survey to examine studies relevant to ''spear phishing,'' and user studies pertaining to ''phishing/spear phishing,'' and categorised the studies pertaining to detection techniques in the existing literature on the basis of the attack vector for which the technique was employed (such as URLs, websites, emails); they also categorised the studies pertaining to user awareness. In addition, they studied the properties of the dataset, feature extraction, detection algorithms, and performance evaluation in order to analyse detection techniques. The study in [26] classified phishing attacks and their corresponding solutions, offering an insight into features that allow distinguishing phishing emails from legitimate ones; they also considered different techniques between the years 2000 and 2016, and made comparisons among 15 techniques aimed at detection of phishing attacks, and another 15 techniques aimed at identification of phishing websites. Moreover, a few dataset sources have been mentioned in [27], whereby a total of 18 proposed solutions have been explained between the years 2000 and 2016; the researchers have also presented a taxonomy or classification of these techniques and mentioned features that help distinguish between phishing and legitimate emails. They evaluated different anti-phishing tools used in research and practice and presented a contrast between them. The researchers identified the gaps by pointing out the attack vectors and communication modes that have been rarely considered in literature. In this context, the survey conducted by Chiew *et al.* [28] in 2018 focused on vectors or channels involved in phishing attacks. The paper discusses how social engineering attacks take place, and the techniques involved therein. Moreover, it sheds light on the possibility of more robust attacks in the future due to a combination of various available techniques.

Can you add one short paragraph here to show the main limitations of the published surveys discussed above? This will be the problem gab of our paper. This should be mainly about phishing email surveys.

A. RESEARCH CONTRIBUTION

The main aim of this study is to systematically review phishing email detection studies that include NLP techniques. Based on specific predefined criteria, a total of 100 research articles published between 2006 and 2022 were analysed. We studied the key research areas in phishing email detection using NLP, ML algorithms and optimisations techniques used in phishing detection email, text features in phishing email, datasets and resources used in phishing email, and evaluation criteria. The survey indicated a complete lack of investigation of systematic literature review on phishing email detection using NLP techniques. Moreover, the survey of the available literature showed that no studies relevant to phishing email detection using NLP techniques addressed Arabic text.

B. PHISHING DEFINITION

The aim and the scope of the approaches to phishing detection can be examined through the definition of phishing that has been presumed by such approaches. The literature includes several definitions of phishing which are summarized in Table 1. It provides definitions by PhishTank [29], the Anti-phishing Working Group (APWG) [30], Xiang *et al*. [31] and Ramesh *et al.* [32]. It presents a comparison of phishing definitions based on the target and phishing strategy. The most leading phishing strategies are social engineering (e.g., through fraudulent emails) and technical subterfuge (e.g., malware infection) [9]. On the other hand, classic techniques (e.g., pharming [33]) are also used to yield personal information about users from the Internet [34]. In contrast, the definitions of Whittaker *et al.* [35] and Khonji *et al.* [25] are not bound to the attacker's target (e.g., sensitive personal information). They define the phishing strategy (e.g., phishing website or socially engineered

messages) without affirming to a precise phishing target (e.g., only state the attackers' benefit). With no scientific agreement, the other sources might deliver a standard definition [36]. In order to initially find the definition of the word, the dictionary is considered the primary source. Table 1 shows three definitions from prominent English dictionaries. Furthermore, it lists the definition of the Anti-Phishing Working Group (APWG), a non-profit foundation that keeps a record of phishing [36]. The definition by APWG is lengthy compared to the dictionary definition. The five definitions differ in the level of detail and scope. For example, the American Heritage definition consists of phone calls, whereas the others do not. Additionally, the aim of phishing varies in the definitions, fluctuating from financial account details (Collins, APWG) to more general personal information (Oxford, Merriam- Webster, American Heritage) [36]. One bank may consider a fraudulent phone call as phishing, whereas another bank may not. Therefore, oppression or countermeasures can be hardly assessed. Consumers may also suffer from the downside of a lack of a standard definition. It is difficult for people who are less computer literate to understand phishing. We aim to clarify the definition of the phishing phenomenon by analysing the already present phenomenon as compared to most of the standard definitions that have already been established by experts. The generated definition is dependent on the consensus that is illustrated through the literature, and is enough for assisting further development. In fact, several academics have characterised phishing since the inception of phishing attacks; however, their interpretations differ and often do not coincide. After reviewing numerous phishing definitions, Lastdrager [36] conclude that ''phishing is an extensible attempt to induce in which imitation is utilized to collect information from a target.'' To summarise this, the definition of Whittaker *et al*. [35] is considered to be the most general, while APWG [30] defines the most frequently used phishing attacks in a precise manner. In the authors' opinion, Lastdrager's [36] definition captures the core characteristics of phishing while also encompassing a broad range of attacking means used by phishers.

As previously stated, a phishing attack begins with an email sent to an online customer. Crimeware is a kind of malware that is defined as software which accomplishes illegal activities that are expected to generate monetary gains for the assailant [37]. The technical subterfuge schemes are generally activated by users' actions like opening an attachment (see Figure 1).

Four steps are normally followed by the malware's activities: betraying a user to activate it, blocking technical defence, attaining its purposes, and lastly propagating [38]. Considering, for example, when a user opens an attachment file in an email, a keylogger can be installed, or when the link is clicked, the user can be readdressed to the phishing website by DNS attacks. So, the main part of phishing is to deceive the users by giving fake information and bait them to achieve actions in favour of foes.

TABLE 1. Most popular definitions of phishing.

Source	Definition	Target	Strategy
American Heritage Dictionary (2013), USA	"To request confidential information over the Internet or by telephone under false pretences in order to fraudulently obtain credit card numbers, passwords, or other personal data".	Personal information	Not specified
Anti-phishing Working Group (2013)	"Phishing is a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data & financial account credentials".	Identity data, financial account credentials	Social engineering
Collins English Dictionary (2013), UK	"The practice of using fraudulent e-mails and copies of legitimate websites to extract financial data from computer users for purposes of identity theft".	Not specified	Not specified
Khonji et al.	"Phishing is a fraudulent act to acquire sensitive information from unsuspecting users by masking as trustworthy entity in an electronic commerce".	Not specified	Social engineering
Lastdrager (2014)	"Phishing is a scalable act of deception whereby impersonation is used to obtain information from a target".	Not specified	Not specified
Merriam-Webster (2013), USA	"A scam by which an e-mail user is duped into revealing personal or confidential information which the scammer can use illicitly".	Personal information	Not specified
Oxford University Press (2014), UK	"The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online".	Personal information	Not specified

TABLE 1. *(Continued.)* **Most popular definitions of phishing.**

PhishTank	"Phishing is a fraudulent attempt, usually made through email, to steal your personal information".	Personal information	Social engineering
Ramesh et al.	"Phishing is a type of computer attach that communicates socially engineered messages to humans via electronic communication channels in order to persuade them to perform certain actions for the attacker's benefit".	Sensitive information	Not specified
Whittaker et. al.	"Phishing page is any web page that, without permission, alleges to act on behalf of a third party with the intention of confusing viewers into performing an action with which the viewer would only trust a true agent of the third party".	Not specified	Not specified
Xiang et al.	"Phishing is a form of identity theft, in which criminals build replicas of target Web sites and lure unsuspecting victims to disclose their sensitive information like passwords, personal identification numbers (PINs), etc...".	Sensitive information	Not specified

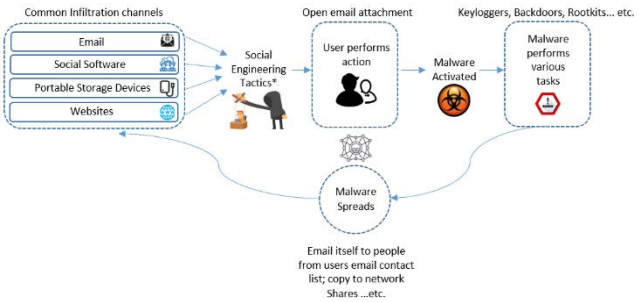

FIGURE 1. **Common channel and strategies used by malware to infiltrate a system (adapted from [38]).**

Phishers offer potential victims with fake situations where the users are advised to execute a specific type of significant activity. Some examples of the typical situations are as follows: a user's webmail storage is almost surpassing the limit, a user's bank account is required to be updated because of some security measures, a user's online transaction has not been managed because of inappropriate information that the user entered while the goods are being purchased, etc. [39].

C. PHISHING LIFE CYCLE

As previously stated, a phishing attack begins with an email sent to an online customer (see Figure 2). This email contains a fraudulent link that redirects the user to a fake website, which is cloned by the attacker to seem exactly like the original website on which it is based. This persuades the gullible email recipient of the email and website's legitimacy. Figure 2 depicts a phishing email and its essential components. This information was acquired from the University of Massachusetts Amherst [40] and aims to help show how to protect internet users against deceit. The features of the fake website are depicted in Figure 3, where the email recipient is required to supply confidential information, which the attacker then obtains and uses illegally.

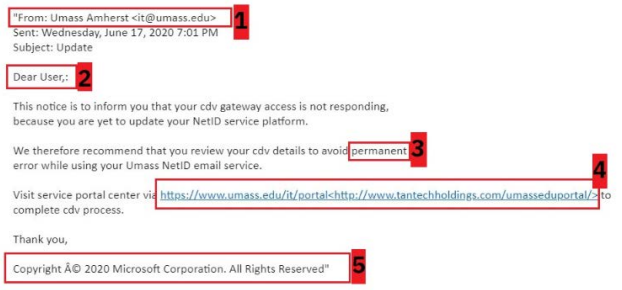

FIGURE 2. **Fresh Phishing email example [40].**

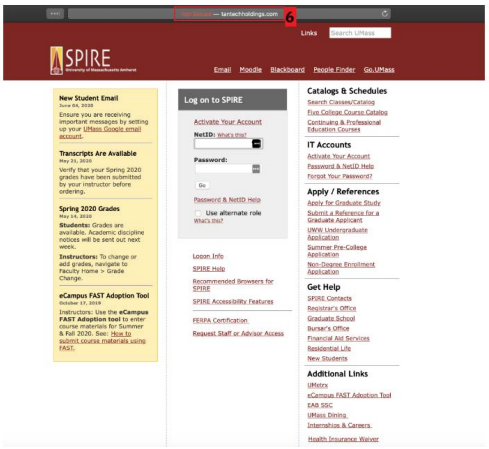

FIGURE 3. **Phishing website with annotations [40].**

1. Despite claiming to be 'UMass Amherst <it@umass.edu>, the sender is actually not associated with UMass and the actual email address isn't one of the university's email addresses.
2. In a phishing email, it's easy to identify spelling and language mistakes. In this email, for example, there is a comma before a colon, which is incorrect.

3. A phishing email will also include language that generates a false feeling of urgency. This prompts the recipient to take action without much deliberation.
   - The threat of a 'permanent' error if the receiver takes too long to act is one example found in this email.
4. The message link is crafted to look like an authentic UMass Amherst page address. However, hovering over it reveals that it leads to a different page.
   - Hovering over a link reveals where it leads, which in this case is not to a trusted UMass website. As a result, double-check the links before clicking them!
5. Another flaw in the mail is that it claims to be from both UMass Amherst and Microsoft Corporation. The sender is a phony if they are unsure of their own identity and affiliation.
6. The link included in the message leads to a fake SPIRE login page with the web address being ''tantechholdings.com''

III. PHISHING EMAIL DETECTION

A. TAXONOMY OF AN EMAIL MESSAGE

Filtering e-mails is a method of distinguishing between legitimate and phishing email messages. This technique uses either a phishing e-mail filter, which examines and categorises e-mails into their appropriate groupings, or a learning-based filter which analyses a collection of labelled coaching data (previously collected messages with upright evaluations) [13], [41], [42]. Another method of analysing e-mail messages is to examine each one individually for the existence of any unique words. E-mails are divided into the body and the header [42]. The e-mail headers contain several fields, such as from, subject, to, and so on [42]. The header lines not only give information about the message's subject, receiver, and sender, but they also give explicit routing data. The body of the email follows the header lines and contributes to the message's content. Figure 4 depicts the structure of an e-mail, and Figure 5 illustrates the structure of an e-mail message for the purposes of feature extraction and selection [13].

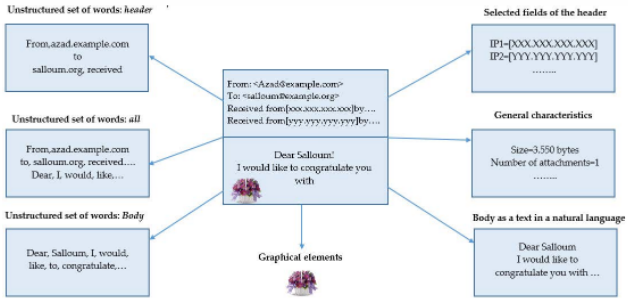

FIGURE 4. Taxonomy of email message structure (adapted from [43]).

To comprehend the various strategies of e-mail filtering, it is critical to gather operating data regarding the format and structure of an e-mail [41]. This also aids in the identification of the pre-processing stage. The employment of envelopes

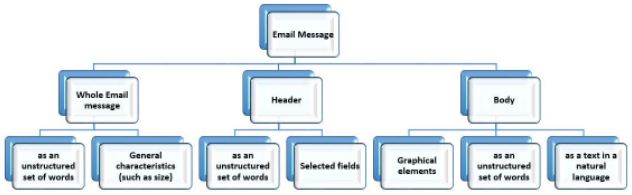

FIGURE 5. An example of the structure of e-mail messages (suggested for purposes related to feature extraction and selection (adapted from [43]).

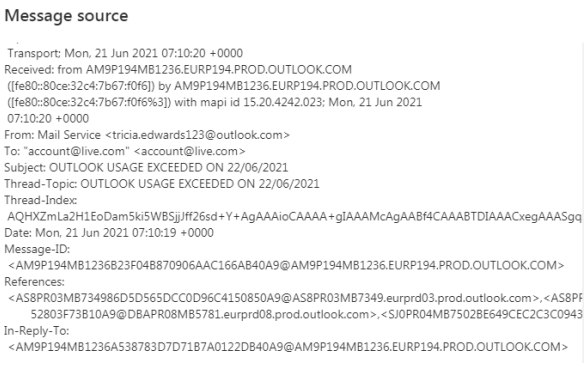

FIGURE 6. E-mail envelope and source code.

in this modern method, similar to ancient communication mail, is an interesting feature. An e-mail envelope is not visible to the naked eye since e-mail systems remove it before delivering the e-mail message [42]. Figure 6 shows an e-mail envelope and source code for an e-mail, respectively.

B. MACHINE LEARNING TECHNIQUES

Figure 7 depicts the various phishing email detection methods utilised in the literature, and also the volume of publications

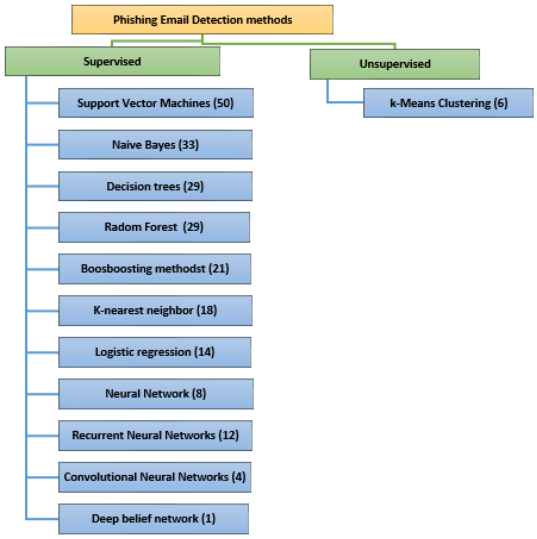

FIGURE 7. Methods used in phishing email detection.

that use each method. The most prevalent phishing email detection algorithms are supervised approaches, such as support vector machines (SVM) [44]–[50], logistic regression (LR) [44], [45], [48], [51]–[56], Decision Tree (DT) [48]–[50], [57]–[62], and Naïve Bayes (NB) [44], [63]–[65]. Unsupervised approaches such as k-means clustering [48], [66]–[70] and deep learning methods have also been adopted [45], [51], [52], [63], [71]–[82].

1) SUPERVISED CLASSICAL ML ALGORITHMS

a: DECISION TREE (DT)

A commonly used ML algorithm that can be applied for regression and classification is the decision tree. A recursive partitioning algorithm is applied to test the availability of attributes or features considering specific purity indexes [83]. The Gini Index and Entropy are the most commonly used indexes, where the former is applied to measure the probability of a randomly chosen feature that is incorrectly classified [49]. The uncertainty amount that is proportional to the information gain is referred to as Entropy [49]. By means of these indexes, the required position of the features, either internal node or root, can be determined. The decision tree can be applied to the categorical or continuous variables. Instances of research in the literature using DT are [48]–[50], [56]–[62], [64], [67], [75], [87]–[101].

b: RANDOM FOREST (RF)

A random forest is an ensemble classifier that makes predictions using a variety of decision trees. It works by fitting a variety of decision tree classifiers to different subsamples of the dataset. In addition, each tree in the forest was constructed using a random selection of the best attributes. At the time of the training phase, the decision trees are created (as defined by the developer), and these are applied for the class prediction use. They are attained through consideration of the voted classes for each specific individual tree, and the class which attains the highest number of vote is considered the output. Similar issues within literature are resolved using the RF method [44], [46], [49], [54], [56]–[58], [61], [71], [73], [84]–[102]. RF details can further be attained using [103], [104].

c: NAÏVE BAYES (NB)

The Bayes rule of conditional probability is applied by this classifier, and all data features are applied. They are individually analysed based on the assumption that they are not only independent but also as important as one another. Quick convergence and simplicity are the classifiers benefits, yet it is not possible to understand the associations and interactions amongst the features of each of the samples. The following papers [44], [50], [53]–[56], [58], [61], [63], [64], [66], [71], [73], [77], [80], [85], [87], [89], [91], [94], [97], [101], [102], [105]–[114] have reported the use of NB to enhance the textual features in phishing email detection.

d: SUPPORT VECTOR MACHINE (SVM)

SVM is usually applied for classification activities as well as regression activities. Each data item within the SVM is plotted as the point within the n dimensional space (n is the feature number for each sample within the training set). The mission of the algorithm is to extract the most appropriate hyper-plane which can be split into two classes. The non-linearly separable data is classified by SVM through transformation into higher dimensional space, with the help of a kernel function, in which a separating hyperspace is present. Yet, it is difficult to interpret the SVM, and it is quite memory sensitive. We noticed that numerous scientific papers, such as [44]–[50], [53]–[56], [58], [61], [63], [66], [70], [71], [73], [80], [87]–[89], [91], [94], [96], [97], [99], [101], [102], [106]–[110], [112], [114]–[128] have used SVM algorithm to detect phishing emails.

e: NEURAL NETWORKS (NN)

The structure of the NN is formed by a set of interconnected identical units (neurons). Through these interconnections, signals are sent from one neuron to another [129]. Furthermore, weights are attached to the interconnections so that delivery between the neurons is enhanced [130]. On their own, the neurons aren't powerful; however, when they are connected, complex calculations can be carried out. At the time of network training, the interconnection weights are updated, therefore, during the testing phase, interconnection plays a significant role. The NN example can be observed in Figure 8. Within the figure, the NN includes "an input layer, hidden layer and output layer." The network is referred to as feedforward as the interconnections do not skip or loop back to the rest of the neurons. The nonlinearity present within hidden neurons helps provide the NNs power. Furthermore, the network must include nonlinearity so that complex mapping can be learnt.

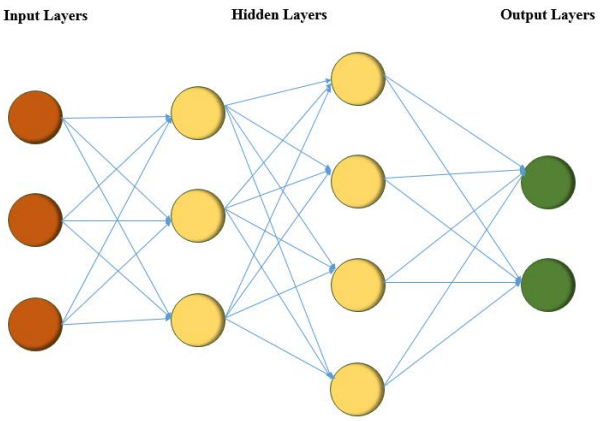

FIGURE 8. Neural network.

The NN model fitting needs experience, even though it is competitive as part of the learning ability. The local minima are quite standard, and there is need for delicate regularisation. Many papers [53], [54], [66], [70], [87], [91],

[94], [102], [105], [111], [112], [131]–[133] have used NN differently.

f: LINEAR REGRESSION (LIR)

Linear regression is a supervised learning machine learning technique. It carries out a regression task. Based on independent variables, regression models a goal prediction value. It is mostly utilized in predicting and determining the link between variables. Few researchers [44], [55] have used LIR to train and test their models to detect a phishing emails.

g: K-NEAREST NEIGHBOURS (KNN)

A commonly applied supervised learning algorithm is the KNN, which usually helps in classification. The assumption here is that similar aspects maintain close proximity. Similarity measures are applied to check for the similarity degree, most commonly the Euclidean distance. Implementation is easy with KNN, as tune parameters and model parameters are not built. The KNN is referred to as a non-parametric algorithm, which is why fundamental assumptions regarding the distribution of data are not required. The algorithm will perform slower based on the increase in size and dimensionality of the dataset. We noticed that several studies, e.g., [44], [46], [49], [50], [54], [55], [57], [60], [62], [77], [82], [88], [89], [94], [96], [97], [107], [112], [134] have used the KNN algorithm in phishing email detection.

2) SUPERVISED DEEP LEARNING ALGORITHMS

Deep learning is an ML branch that uses multilayer artificial neural networks (ANNs) to achieve state-of-the-art accuracy in complicated problems such as computer vision [135]–[137], speech synthesis [138], [139] and recognition [140], [141], language translation [142], and several others such as fraud detection [143], [144]. Deep learning differs from classical ML methods, in that it has the unique capacity to learn depictions instantly from a variety of data types like audio, video, text, or images without the requirement for hand-written constraints or subject technical expert knowledge. Because of the adaptable design, they can learn straight from raw data and improve prediction accuracy as more information is available. GPU-powered inference systems are necessary to improve performance and provide low latency inference'' for the computationally demanding deep neural network (DNN) The most often used deep learning models are CNNs and RNNs.

a: CONVOLUTIONAL NEURAL NETWORK (CNN)

Various convolutions layers along with nonlinear activation function such as ReLU are referred to as the CNNs. As compared to the traditional NN where the layers are fully connected, the CNN convolution upon the input is carried out for computation of the output, and it provides the outcome of a local connection. For each layer, there is a significant number of filters that are applied, and its output is combined to attain outcomes. At the time of the training phase, the CNN learns filter values. In the case of NLP tasks, the CNN input are documents or sentences. A matrix row is used to represent the character or word, and this provides the vector which is aligned to the word, referred to as word embedding. The matrix column space is stated by the embedding dimension. The CNN differences amongst NLP and image is the choice of filter and size. For images, the filter is the slide over the input's local patch, but in NLP it will slide over the complete row, as the word is represented entirely. Hence, the filter matrix column space would be similar to the input matrix column space [145]. We noticed that several studies, e.g., [45], [63], [74], [75] have used the CNN method.

b: RECURRENT NEURAL NETWORK (RNN)

The hidden sequential associations in variable-length input sequences are learned by a RNN, which is mostly utilised for sequential data modelling. Many noteworthy successes in the areas of NLP and speech synthesis and recognition can be attributed to recurrent NN methodologies [52]. The RNN, on the other hand, has a long-term dependency issue, which could exacerbate the gradient exploding and vanishing issues. Polymorphisms of RNN have been developed to overcome the difficulties with it, one of which is the long short-term memory (LSTM) [81], [146]. To achieve the goal of learning this ''long-term dependence'' data, the LSTM utilises gates on the input and recurrent input to influence the state and also output at multiple intervals.

Similar to the convolutional network, the LSTMs needs the same size inputs, hence, for the network input, it is only necessary to have the initial N email words [63]. RNN have been utilised by several academics [45], [51], [52], [63], [78]–[82] to train and test their phishing email detection models.

3) UNSUPERVISED LEARNING ALGORITHMS

a: K-MEANS CLUSTERING

The technique applied for dataset partitioning or clustering into k groups is referred to as cluster analysis. Random selection of the k data points (clusters) is done and then passed through an iteration series using the mentioned methods.

1. For a specific word, w, they will be aligned to the closest cluster centre Cj with $1 \leq j \leq k$.
2. Each cluster centre (Cj) value will be updated using the mean value from the words that are part of the cluster [147].
3. Till the time the cluster cannot be changed any further, the algorithm will continuously run.

Usually, topic modelling, ''term frequency–inverse document frequency (TF-IDF)'' and clustering procedures like the k-means are complementary, and may be used integrated, specifically the TF-IDF vectorisation as the precursor to k-means clustering, in order to present an in-depth assessment [69]. Earlier research studies, like Ruiz-Casado *et al.* [148] and Rong [149] have been carried out with the help of Wikipedia keywords to indicate that

the TF-IDF vectors and clusters of words outcomes are strictly aligned with the groups expected, allowing them to be an effective article classification tool [69]. NLP, topic modelling, and clustering techniques were combined to analyse and assess the persuasive techniques/strategies used by cybercriminals when fraudulent emails are created (Stojnic *et al.* [69]).

The experimental results indicate that when these techniques are applied, it is possible to understand the mindset of the cybercriminals along with the ability of the techniques to attain consistency, even though there has been a strategy evolution from early scams towards the modern phishing emails.

C. FEATURE EXTRACTION

Feature extraction is the process of converting raw data into numerical features that may be processed while maintaining the information in the original data set. It yields better results than just applying machine learning to raw data [150]. There are some techniques to extract features from text like principal component analysis (PCA) and latent semantic analysis (LSA), in which the input data is DTM, keeping in mind the TF-IDF measure (F). The following are the primary perspectives.

1) PRINCIPAL COMPONENT ANALYSIS (PCA)

PCA, as stated by [151], aims to extract mapping from within inputs of the original dimensional space towards the developed smaller dimensional space, ensuring minimum information loss [54]. Using the available data structure, it is possible to understand the structure and extract them through eigenvectors and eigenvalues, which help maximise the projected data variance and spread them out over the new dimensional space [54]. The objective of the technique is to alter the variables that can be correlated, into the linearly uncorrelated variables and the principal components by applying the orthogonal transformation, as stated by [152]. The principal component direction is represented by the eigenvectors, and the direction variance is brought forward by the eigenvalues. We noticed that several studies, e.g., [54], [56], [66], [89], [109], [153] have used the PCA technique in phishing email detection.

2) LATENT SEMANTIC ANALYSIS (LSA)

For NLP, the mathematical procedure applied is the LSA. Its objective is to embed the topics within the input data (documents) explicitly, extracted from the highest values, and attained based on the feature number required [54]. Removal is conducted for the features not selected and having values lower than the threshold value. They are not used in the following activities. The input data for chi-square and the mutual information measures is DTM, keeping in mind the TF-IDF measure, (F) are applied. These are univariate feature selection procedures [54]. The initial one is the chi-square to measure the linear dependency amongst the two random variables (input feature and target). The second is the mutual information, which integrates the nonlinear associations amongst input features considering target and analysis [54]. Many studies [54], [66], [153] have used LSA differently.

3) CHI-SQUARE

A commonly used feature selection procedure is the chi-square ($\chi 2$) [154] which assesses individual features through computation of chi-square statistics within the context of classes. Hence, the chi-squared score can analyse the term and class dependency [155]. If the class and term are independent, then the score would be 0 otherwise 1 [155]. The score is informed depending on the term having a high chi-square. We observed that some studies, e.g., [54], [153] have used the Chi-Square in phishing email detection.

4) MUTUAL INFORMATION/INFORMATION GAIN

The measure used for the quantification of mutual dependence amongst two variables is mutual information. It is based upon random variable entropy (within information theory). Through mutual information, the information amount that is attained within the random variable is calculated, using a different random variable. Considering the work proposal, the information of each feature is identified, thereby stating whether the email is phishing or legitimate [152].

A procedure that uses the information gain measure to rank features can be used to select the most useful features [156]. For the metric, a threshold is then decided, and the attributes are kept with a value attached—only the top-ranked ones are kept. Furthermore, the features are selected by information gain through scores. Such a technique remains simple as compared to the earlier. The concept is that each feature score is computed, which then indicates the class discrimination and the features are then sorted based on the score. The top-ranking ones are the only ones retained. Mutual information has been utilised by several researchers [54], [113] to extract/select the features in phishing email detection.

D. TOOLS AND TECHNIQUES

This section discusses the numerous tools used for experimental purposes as well as the evaluation of an anti-phishing system's accuracy. A researcher's tool selection is influenced by a variety of parameters and algorithms. Figure 20 shows several tools that can be used for phishing detection evaluation. Python is the most commonly used one for phishing email detection [8], [17], [33], [36]–[39]. Table 2 delves deeper into these tools and their uses in many sectors.

E. EVALUATION METRICS

A confusion matrix depicts a table that shows a general summary of the classification and segmentation performance. Furthermore, certain binary classification problems need a two-group confusion matrix which is often utilised to present the positive and negative classes. There are four groups of the matrix included in this study, as follows: False negatives (FN), false positives (FP), true positives (TP) and true

TABLE 2. Most popular tools of phishing detection.

No.	Tool	Description
1	Python	One of the easiest to learn and most valuable programming languages is Python. Python is a sophisticated language with enhanced data structures and a straightforward approach to object-oriented programming. Its refined syntax, dynamic typing, and interpreted semantics make it a perfect language for scripting and quick application development across a variety of platforms [157].
2	WEKA	WEKA is a tool that provides a graphical user interface (GUI) that aids the functions of an algorithm by allowing the user to import a dataset and apply various functions/rules to the algorithm [158]. As a result, categorisation, regression, and grouping of algorithms are possible, as well as data visualisation and algorithm performance.
3	KERAS	Keras, a NN API, works with deep learning algorithms to provide simple and quick techniques [102], as well as CPU and GPU running features so models may be processed simultaneously.
4	TensorFlow	TensorFlow is a Google-developed end-to-end ML platform that allows users to run programs on multiple CPUs. This program includes GPU access, and the website is user-friendly for beginners as well as a learning tool for professionals [102]. TensorFlow can be readily combined with Keras to conduct deep learning experiments [159].
5	SCIKIT-LEARN	It is a library environment that provides not only a large selection of supervised algorithms appropriate for the project at hand [102], but also high-level implementation to train using 'fit' methods and 'predict' via an estimator or a classifier. Cross-validation, feature selection, feature extraction, and parameter tuning are among the other features available in this program [160].
6	NLTK	The Natural Language Toolkit, also known as NLTK, is a tool that generates interfaces for text processing, access to huge corpora collections, and linguistic structure. It is a Python package for NLP [161] that comprises libraries and programmes for parsing, chunking, tokenisation, PoS tagging, semantic analysis, clustering, and classification, among other NLP functions.
7	MATLAB	MATLAB is a high-performance technical computing language which combines features like computation, visualisation, and programming in a user-friendly environment whereby the issues and their solutions are written in recognisable mathematical notations [162].

negatives (TN), as displayed in Table 3 [163]. These can be utilised to attain the four measures of classification performance. The complete negative incorrect predictions represent FN, the complete positive incorrect predictions represent FP, complete positive correct predictions represent TP and complete negative correct predictions represent TN.

$$\text{Precision} = \text{TP}/(\text{TP} + \text{FP}) \quad (1)$$

$$\text{Recall} = \text{TP}/(\text{TP} + \text{FN}) \quad (2)$$

$$\text{F1-measure} = 2 \times ((\text{Precision} \times \text{Recall})/(\text{Precision} + \text{Recall})) \quad (3)$$

$$\text{Accuracy} = (\text{TP} + \text{TN})/(\text{TP} + \text{FP} + \text{TN} + \text{FN}) \quad (4)$$

To perceive these measures, the confusion matrix provided in Table 3 can be assessed.

TABLE 3. Confusion matrix.

Confusion matrix	Predicted positive	Predicted negative
Actual positive	TP	FN
Actual negative	FP	TN

There are some more metrics recorded in certain papers, for instance, area under curve (AUC), and receiver operating characteristics (ROC) [51], [55], [59], [61], [87], [92], [98], [132], [153], [164]. Moreover, when taking into account imbalanced datasets, the utilisation of relevant evaluation metrics is an essential aspect with which to reckon. There are some grounds on which accuracy is unsuitable, for instance, asymmetric costs, base-rate fallacy, and imbalanced datasets. The same situation is seen with the ErR metric and in this plan, the preferential values should be the confusion matrix, ROC, and AUC. In addition, the metrics particularly suggested for imbalanced investigations must be utilised by the researchers [165], for instance, balanced accuracy, Matthews correlation coefficient (MCC), geometric mean, and balanced detection rate, and others. Although, certain papers utilise greatly imbalanced URL datasets, [166], [167], error rates [117], [125], make use of detection rates and malicious missing rates [168], and employ metrics in demand such as recall, $F1$-score, accuracy, precision, and ROC [169] utilising FP and FN rates, when the class grouping and dataset size is recorded, they can have an advantage of working out different metrics. Therefore, in the literature studies, mainly unsuitable imbalanced dataset metrics were noticed [10].

F. DATASET PROPERTIES

The datasets utilised by the authors in order to test and train their models carry a vast impact on the credibility of their models, even though an essential feature of a suggested system is the detection process. Furthermore, the datasets utilised in website detection are nearly similar to the one utilised in the email detection methods, hence revealing the absence of a variety problem. In order to train/test the models, sometimes malware and spam emails are used, even though the papers are only regarding phishing email detection. These types of papers are categorised in the *malicious* class (*spam* dataset represents URLs taken from the body of spam emails).

The author's research contains papers with personal data sources of the researchers. If the information regarding their sources is not disclosed, they are recorded as the author's private information, or are recorded as the author's public information, if it is released. The papers that contain legitimate, phishing, and malicious sources are listed in Appendix Table A2.

The ground truth datasets are utilised by the different approaches, which they gather it from various cyber

TABLE 4. Dataset features.

No.	Dataset feature	Description
1	Dataset source	The generally utilised data sources of legitimate and phishing websites along with the approaches that grip every source are mentioned in Appendix Table A2. However, the insufficient understanding regarding the methodologies utilised in the collection and preservation of every source results in no concord at all in terms of the quality of various sources.
2	Dataset size	The evaluation dataset size differs between various approaches. As seen, the reliable outcome depends on the size of the dataset; the bigger the better
3	Dataset redundancy	There is not sufficient information in the literature regarding datasets redundancy. Although numerous presentations and overlay between various sources of datasets, particularly of phishing websites, can be seen.
4	Dataset timeliness	Although if a similar source of data and size of the dataset is utilised in two plans, their phishing website information might not be the same. The phishing blacklist supplier generally amends their data plan weekly, daily, or even hourly, because phishing websites last for short-terms.
5	Ratio of legitimate to phishing websites	The ratio of legitimate to phishing example displays the level at which experiments portray an actual world distribution (≈ 100/1) [9].
6	Training set to testing set ratio	The extensibility of the approach is seen in the ratio of training to testing examples [9].

intelligence sources, and the evaluation is firmly combined with it. In addition, there are various testing methodologies which are been used by these sources. These sources also target various kinds of phishing activities, therefore shield various phishing domains. As seen, there is a contrast between the evaluations relying on one dataset from another. For this reason, there is a debate on how essential it is to have a publicly available reference dataset in order to classify the evaluation of different approaches. Moreover, this essential part can present a benchmark in order to contrast the efficacy of different approaches, and eventually make it easier for the analyst to make improvements in the field in an additional systematic manner. However, the rerun of experiments for the systematic contrast of efficiency is difficult to achieve due to the missing of reference sets along with the complexity of code sharing. The determining features of the datasets utilised in the literature are listed in Table 4.

G. DATASETS USED FOR EVALUATION

Several datasets employed for the evaluation of phishing detection algorithms are available freely on the internet. Some of the most renowned phishing and ham datasets are summarised in Table 5.

H. OPTIMISATIONS TECHNIQUES

The term 'optimisation' alludes to a method for determining the input parameters or arguments to a function that produces the function's minimal or maximum output. Continuous function optimisation, in which the input variables to the function are numeric is the most prevalent form of optimisation problem faced in ML. The function's output is a real-valued assessment of the input parameters as well. To separate these challenges from functions that take discrete variables, and are alluded to as combinatorial optimisation issues, we may call them continuous function optimisation issues. The population optimisation algorithms are stochastic optimisation algorithms that keep a pool (a population) of potential solutions that is utilised to select, examine, and narrow in on an optimal solutions. This sort of algorithm is designed for more difficult unbiased issues with noisy function assessments and multiple global optima (multimodal), when choosing a suitable or satisfactory adequate approach is difficult or impossible using other approaches.

In phishing email detection, optimisation algorithms have been used in several studies: [47], [52], [57], [59], [68], [70], [102], [105], [115], [126], [127], and the most important of them is the bio-inspired computing (BIC) optimisation technique [185]. The attributes of self-correction and enhancement are inherent in Bioinspired computing (BIC) algorithms, along with a natural tendency to adjust according to the consistently changing environments. BIC is capable of offering flexible, efficient and multifaceted computational algorithms. BIC algorithms have been used in different fields in the past few years to solve issues. BIC solution can be obtained by selecting appropriate dimensions of the problem, assessing the significance of the comparative solutions and describing the operators. Research is being carried out on BIC processes to resolve complicated computational problems [186].

Because each situation is unique, BIC algorithms necessitate various algorithm-dependent parameters [185]. Further BIC may require a high number of iterations to optimise the objective function, which can be inefficient. These algorithms, on the other hand, have two major advantages; the first is an effective information-sharing technique aiding the algorithm's quick convergence, and the other is a lesser probability of becoming trapped in a locally best solution [185]. Other benefits of utilising BIC include the detection of previously undiscovered patterns and a lower reliance on mathematical modelling or extensive training [187]. Several BIC methods have been employed in the literature to find solutions for phishing email detection [47], [102], [126]. One algorithm known as grey wolf optimisation (GWO), which is based on the natural hunting behaviour of grey wolves. Another optimisation technique is chicken swarm optimisation (CSO), which is based on the behaviour and lifestyle of roosters, hens, and chicks in a chicken swarm. Firefly optimisation

TABLE 5. Most popular dataset.

No.	Dataset	Description
1	Phishing Archive	Phishing Archive is an archive of phishing attacks maintained by the APWG. The attacks recorded in this archive were either reported to or detected by APWG [170]. The evaluations of Dhamji et al. [171] and Abburous et al. [172] make extensive use of this dataset.
2	PhishTank	The phishing data reported by the user is stored in the PhishTank website. This information is accessible via API [173] and is shared via a website.
3	Corpora	There were, initially, two components of corpora of the SpamAssassin project: easy ham, as the name suggests, were easily differentiated from spam, and hard ham which were hard to distinguish from spam [174]. There has been a new addition to this corpus in the form of easy ham_2, a ham dataset, spam_3, and a spam dataset [26]. This dataset has been employed by both Fette *et al*. [118] and Khonji *et al*. [175] to evaluate the algorithm PILFER and implement the LUA algorithm, respectively.
4	Enron dataset	Personal emails are included in the Enron dataset [176], which was generated by 150+ employees involved in project CALO [177]. The dataset had integrity difficulties at first, but Bryan Klimt and Yiming Yang [178] were able to repair them. It is regarded as a benchmark dataset, because it contains about 50,000 spam and 43,000 ham emails [26]. The collection of ham messages involves six Enron workers and the TREC 2005 Spam Track public corpus [26]. Georgala *et al*. use the Enron dataset as well for their research [179].
5	TREC	The TREC corpus [180], utilised by Al-Daeef *et al*. is another extensively used dataset [26]. The copyright of this dataset is held by the Waterloo University. The TREC 2005 corpus, which contains 92,189 emails arranged chronologically, and was generated for spam evaluation [26]. There are 39,399 legitimate emails and 52,790 spam emails in the collection. TREC 2006 and 2007 can also be found on their respective websites [26].
6	IronPorts	IronPorts is a defensive mechanism devised by Scott Banister and Scott Weiss in 2000 against Internet threats. In 2007, the Iron Port's corpus [181] was taken by Cisco and has also been employed by Moore *et al.* [182]. A dataset is a collection of data that appear in their spam traps and emails sent to them by consumers. Iron Port's SpamCop [183], created by Jullian Haight in 1998 and acquired by Iron Port in 2003, is a service that keeps track of spam reports from commercial email or UBE recipients (Unsolicited Bulk Emails) with several spam traps in various areas, making it a significant contributor to the Iron Port corpus [26]. SpamCop also analyses all of the reported spam and compiles a list of the systems that were used to send the emails that SpamCop blacklisted [26].
7	Phishload	Phishload is a phishing database produced by Max-Emanuel Maurer in 2012 [184]. Apart from comprising around a thousand legitimate websites, it also contains HTML code, URL, and other data relevant to phishing websites [26].
8	Nazario/Phishing Corpus	The Nazario/Phishing Corpus consists of 7315 emails that were initially collected from 2004 to 2007 and last updated in 2015. The dataset has been used mainly for phishing email detection.
9	SMS Spam Collection	Is used as the public set of the SMS labelled messages, with 5,574 tagged (ham/spam).
10	The Spambase Data set	The UCI data repository of the Spambase Data set has 57 features and 4,601 instances (2,788 emails labelled as spam and 1,813 ham emails) [26]. Mark Hopkins, Erik Reeber, George Forman and Jaap Suermondt from the Hewlett Packard Labs established the dataset [26].
11	Csmining	This dataset includes the emails from six Enron employees extracted from the Enron corpus. One thousand emails were formed and divided into 20% spam and 80% ham. Selection is made from the Enron dataset as it attains a mix of official and personal emails. It does not include the problems present in the rest of the email datasets.

algorithm (FOA) is the third method, and it works by measuring the attraction of fireflies by their flashing behaviour. The ''grasshopper optimisation algorithm (GOA)'' simulates and mathematically models the behaviour of grasshopper swarms in nature [185]. Whale optimisation algorithm (WOA), which simulates humpback whales' hunt for prey, encircling prey, and bubble-net foraging behaviour [185], is also included in the study. Figure 15 shows how often these methods are used in studies in phishing, suggesting that there is scope for further research in adoption of these optimization methods.

IV. METHOD

The guidelines followed for performing a systematic review for the current review study can be found in [188]. The following four phases were employed to conduct the review: ''identification of inclusion and exclusion criteria, data sources and search strategies, quality assessment and data coding and analysis'' [188]. The following sub-sections present the details of these phases. The systematic literature review techniques mentioned in [189] were also followed for this study for better organisation. The introductory procedure of establishing a review protocol is included in the acquired SLR method, whereas planning, carrying out and analysing the review are included in the review process. The following steps were used to conduct the review. The search was identified, the work quality was assessed, the main research was selected, the data was synthesised, the review was recorded, the data was extracted and finally, a verification was performed.

The six steps of the review protocol that are used in this survey are presented in Figure 9. In addition, the research question synthesis is an essential segment of the SLR approach since, at the beginning, it determines the terms of reference for this study. Then, the step that includes combining a search strategy that focuses on establishing the initial studies is

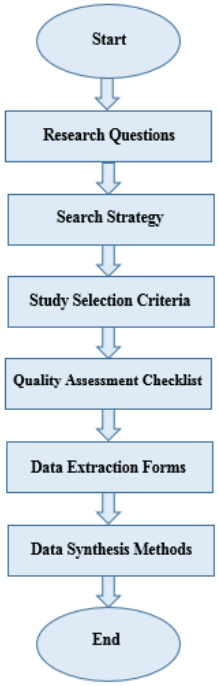

FIGURE 9. Protocol review stages [189].

highlighted in Figure 9. Although this phase is achieved, there should be a way of defining the search terms/criteria and the initial studies must be related to the SLR.

A. INCLUSION/EXCLUSION CRITERIA

The review study will involve the analysis of the articles that fulfil the inclusion as well as exclusion criteria stated in Table 6.

TABLE 6. Inclusion and exclusion criteria.

Inclusion Criteria	Exclusion Criteria
Must involve phishing email detection.	Articles without "phishing email detection" aim.
Must involve NLP techniques.	Articles without NLP techniques.
Must be written in English language.	Articles published in languages other than English.
Must be published between 2001 and 2021	

B. DATA SOURCES AND SEARCH STRATEGIES

The ACM Digital Library, Emerald, Google Scholar, IEEE, ScienceDirect, Springer, Taylor and Francis Online, and Wiley Online Library databases were used to explore and identify the research articles for inclusion in this systematic review. December 2020 marks the commencement of the search for the studies to be included in this systematic review. Search terms used during the search for relevant studies were based on keywords stated in Table 7. Appropriate selection of keywords is imperative for the selection of articles for inclusion in the review, since these keywords serve as the basis for access to relevant articles [190]. The search results obtained through the use of the previously stated keywords led to 1125 articles (see Table 8), including 315 duplicate articles which were excluded through filtration. Consequently, we obtained 810 articles. Each study was evaluated by the authors against the inclusion and exclusion criteria, with 100 articles fulfilling the inclusion criteria, which were subsequently included in the analysis process. ''The preferred reporting items for systematic reviews and meta-analysis (PRISMA)'' was followed during the searching and filtration stages of the articles for the current review study [191]. The PRISMA flowchart is depicted in Figure 10.

TABLE 7. Keyword search.

Keyword search
"Phishing" or "Malware" or "Malicious" or & ["detection" or "approaches" or "methods" or "attack"]
"Phish email" or "Malware email " or "Malicious email" & ["detection" or "approaches" or "methods" or "attack"]
"Phish e-mail" or "Malware e-mail " or "Malicious e-mail" & ["detection" or "approaches" or "methods" or "attack"]

TABLE 8. Final search results across the databases.

No.	Database	Count
1	ACM Digital Library	69
2	Emerald	20
3	Google Scholar	348
4	IEEE	174
5	SAGE Pub	21
6	Springer	266
7	ScienceDirect	171
8	Taylor and Francis Online	15
9	Wiley Online Library	41
	Total	**1125**

C. QUALITY ASSESSMENT

The factor of quality assessment is as important as the inclusion and exclusion criteria [192]. Seven criteria stated in the quality assessment checklist were employed for assessment of quality of the research articles qualified for inclusion in further analysis after filtration (N = 100). Figure 11 shows the quality assessment checklist. The checklist was a modified form of recommendations of [188]. A 3-point scale was taken as a standard for scoring the questions, whereby 1 point was assigned to 'Yes'; 0 points assigned to 'No' and 0.5 points assigned to 'Partially.' The range of points that could be scored by any study was 0 to 7. The greater the total score acquired by the study suggested a higher degree of the ability of the study to give responses for the research questions. The outcomes obtained from the quality assessment of each study are shown in Appendix Table A8, which indicates the fulfilment of quality assessment criteria by all studies, thereby suggesting the eligibility and qualification of all 100 studies in further analysis.

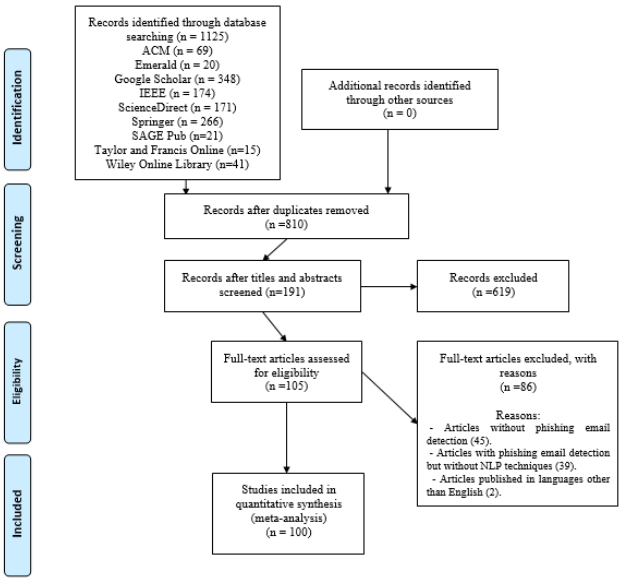

FIGURE 10. PRISMA flow diagram.

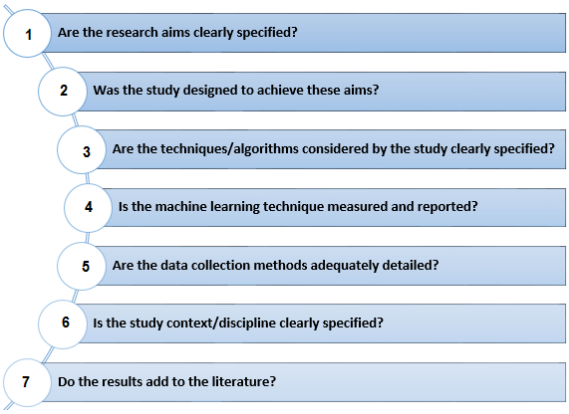

FIGURE 11. Quality assessment checklist [193].

D. DATA CODING AND ANALYSIS

For each study identified, the following information was recorded (a) year of publication (b) the main key research area in phishing detection using NLP techniques (c) research techniques (e.g., AdaBoost, Bayes Net, CNN, etc.), (d) optimisation techniques (eg., Adam optimizer, Cuckoo search algorithm, etc.), (e) text features, (f) NLP techniques used in phishing email detection studies, (g) datasets and resources, (h) evaluation criteria, (i) tools used in phishing detection email using NLP studies, (j) and the parts of the email most widely used in phishing detection email, using NLP studies.

E. PHISHING EMAIL DETECTION STUDIES DISTRIBUTION ACROSS VARIOUS PERSPECTIVES

The current systematic review considered 100 research studies published between 2006 and 2022 on the topic of phishing email detection using NLP techniques, to find answers to 11 research questions which are considered below.

1) **RQ1:** Which ones are the key research areas in phishing email detection using NLP studies?

The main research area in phishing detection studies is feature extraction/selection with 86 studies. Phishing email detection is another significant research area with 68 studies, while 33 studies investigated the classifications of phishing emailx, as shown in Figure 12. Only 14 studies were on improving/optimising algorithm topics, which shows that this research area is not as significant as compared to the other three areas in phishing detection studies, as illustrated in Figure 12.

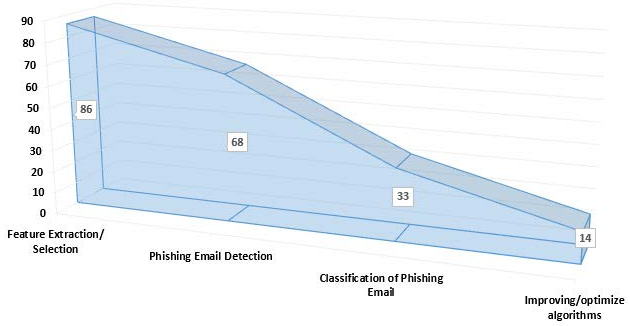

FIGURE 12. Research area distribution.

2) **RQ2:** What are the ML algorithms used in phishing detection email using NLP studies?

Figure 13 shows the distribution of all the analysed articles over the key research techniques in phishing detection studies. The most common research technique used in studies includes support vector machines (SVMs) which have been used in 50 studies. The next most common research technique used is Naïve Bayes (NB), used in 33 studies. This is followed by decision tree (DT) and random forest (RF) with 29 occurrences for each study. Artificial RNN, and NN and CNN are the most applied deep learning techniques, occurring in 13, 8, and 5 studies, respectively. Figure 14 illustrates a summarised view of a 'sample' of 30 techniques drawn from the ML-based techniques discussed in this section. Out of these 30 techniques, nine are supervised, two are unsupervised, and 19 are semi-supervised.

3) **RQ3:** What are the optimisations techniques used in phishing detection email using NLP studies?

Figure 15 illustrates the most popular optimisation techniques used in phishing email detection studies. The most frequently used technique is the Adam optimiser, constituting more than 26% of the optimisations techniques in the reviewed literature. Second in popularity is the sequential minimal optimisation (SMO), with 21% instances of use in the papers reviewed. SMO reveals the significance of a word to a document in the textual datasets.

4) **RQ4:** what are the text features in phishing email detection using NLP studies?

Figure 16 shows the text features used in phishing email detection studies include the bag-of-words (BoW) and

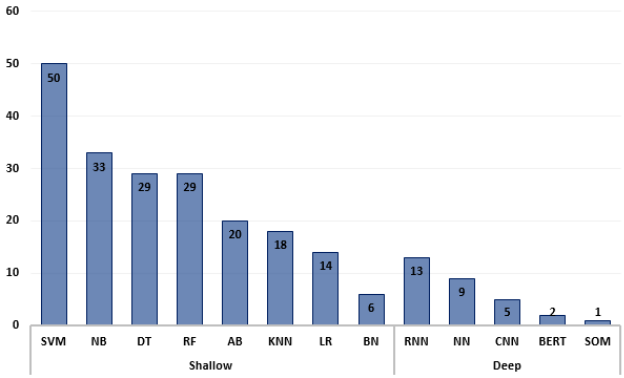

FIGURE 13. The popularity of various ML-based techniques.

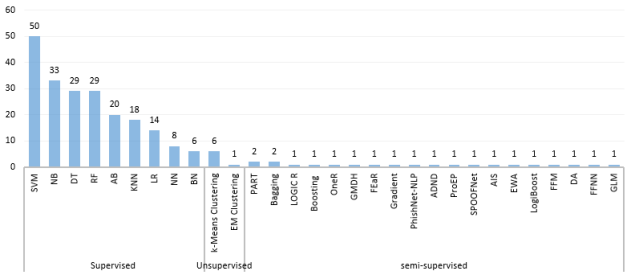

FIGURE 14. The popularity of various techniques.

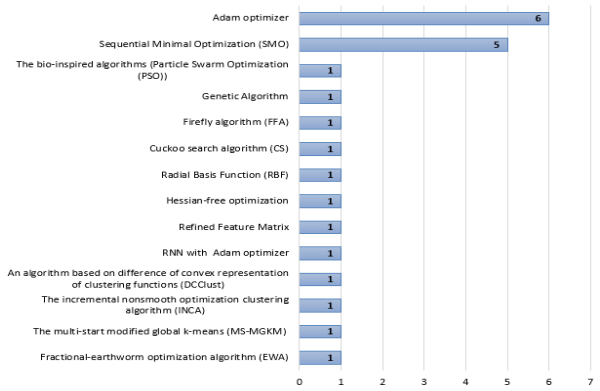

FIGURE 15. The popularity of various optimizations techniques.

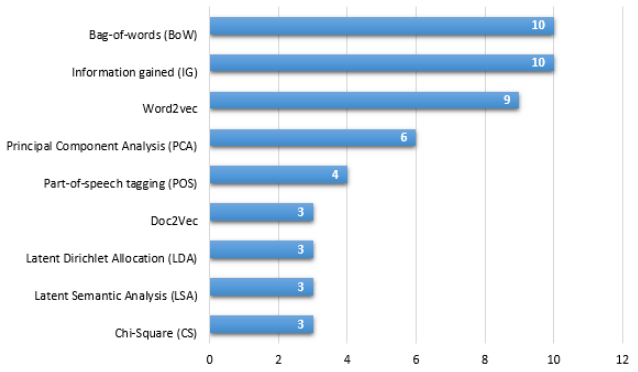

FIGURE 16. The popularity of various NLP techniques.

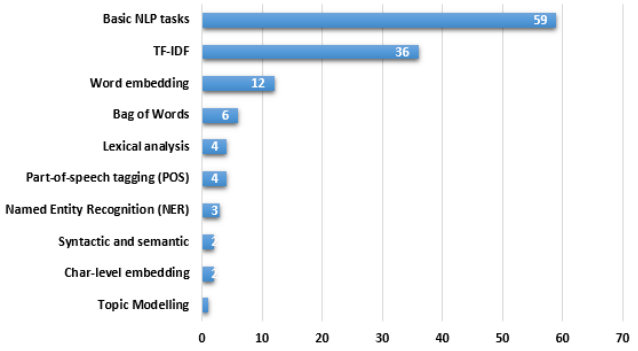

FIGURE 17. The popularity of various techniques.

information gained (IG) that have been used in 10 studies each and Word2vec has been used in nine studies. Other less common but significant features used in studies were principal component analysis (PCA), part-of-speech tagging (POS), doc2vec, latent dirichlet allocation (LDA), latent semantic analysis (LSA), and chi-square (CS), identified in six, four, three, three, three, three studies, respectively.

5) **RQ5:** What are the NLP techniques used in phishing email detection studies?

In terms of NLP techniques, Figure 17 depicts the most popular NLP techniques used in phishing email detection studies. The most frequently used technique is Basic NLP tasks at 59 studies; the basic NLP tasks include '*stopword removal, punctuations, special characters, stemming, and tokenisation*.' Second in popularity is TF-IDF at 36 studies. TF-IDF reveals the significance of a keyword to a document in the textual corpus. Finally, word embedding was found in 12 studies. See Appendix for details.

6) **RQ6:** Which datasets and resources have been used?

Figure 18 shows the distribution of the analysed articles over the resource type. The Nazario phishing corpus has been in the majority of studies at 42 studies. The next common resource is the SpamAssassin Public Corpus, identified in 40 studies. The Enron dataset has also been discussed in 23 studies. This is followed by PhishTank, IWSPA-AP, and TREC corpus at seven, six, and six studies, respectively.

7) **RQ7:** What are the evaluation criteria of the machine/deep learning techniques that were used in phishing email detection using NLP studies?

According to [9] accuracy, precision, recall, and F1-score are the four machine/deep learning methods that serve as metrics for the evaluation of the quality of outcome obtained from various phishing detection techniques [9]. The popularity of applying various machine/deep learning methods as evaluation metrics for phishing email detection has been shown in Appendix Table A1. Multiple metrics were also used in some experiments for evaluation of the quality of the phishing email detection employed. Eighty-three experiments were performed, where researchers opted for

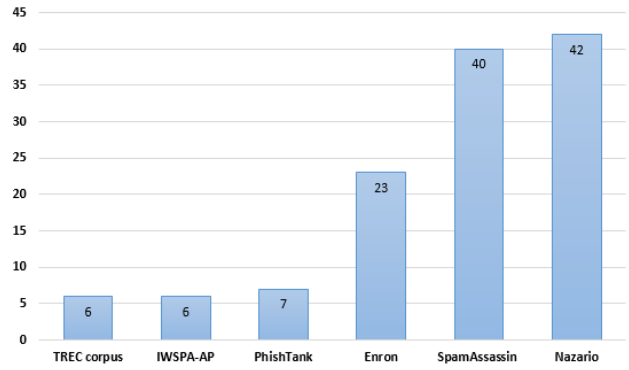

FIGURE 18. Resources type among selected papers.

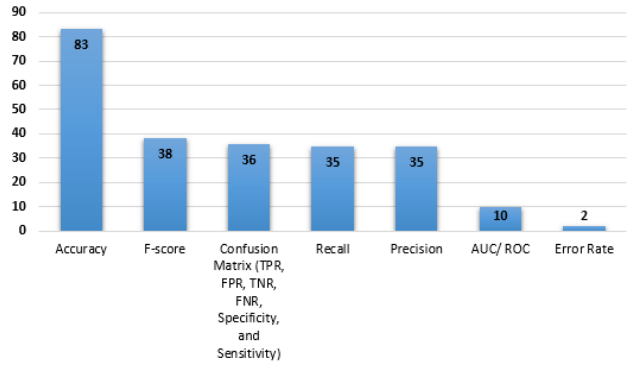

FIGURE 19. Popularity of various evaluation criteria in researches.

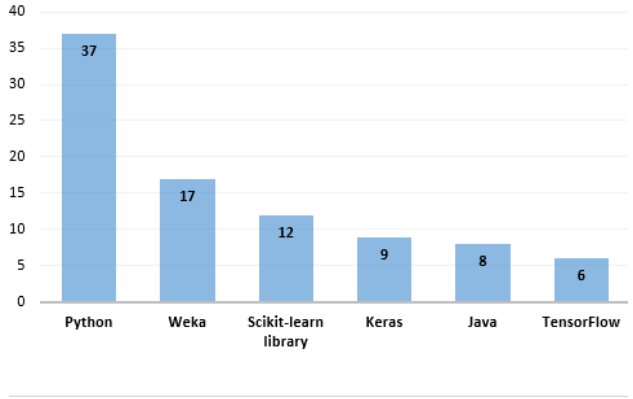

FIGURE 20. Popularity of various tools in researches.

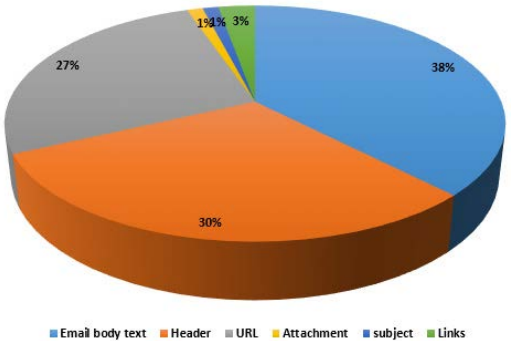

FIGURE 21. Distribution of phishing email detection studies per part of the email.

employing the accuracy standard as a metric, while 38 experiments employed the F1-measure. The metric holding 3rd place in popularity was the confusion matrix (TPR, FPR, TNR, FNR, specificity, and sensitivity, which was used in 36 experiments while the metric of recall and precision standards, used in 35 experiments each, held fourth place, as depicted in Figure 19. It has been found that the measurement of examined classifiers in terms of their quality is done based on accuracy, recall, F1-measure, precision, sensitivity, and specificity. Their computation is shown subsequently. Moreover, any other information regarding the clarification of these measures using a confusion matrix can be viewed in Appendix Table A1.

8) **RQ8:** What are the tools used in phishing detection email using NLP studies?

In this section, we describe popular tools that were used for phishing email detection. Figure 20 describes tools/applications used in the reviewed articles. General tools were collected by the authors of each study. For instance, we have the Python programming language [194], Weka [195], Keras library for the training of deep-learning models, Scikit-learn library, and Java programming language. It can be clearly seen that most of the surveyed studies were conducted using Python (N = 37), followed by Weka (N = 17), then Scikit-learn library (N = 12), Keras (N = 9), Java (N = 8) and TensorFlow (N = 6).

9) **RQ9:** Which parts of the email are the most widely used in phishing detection email using NLP studies?

Figure 21 shows that 38% of the phishing detection email studies mainly relied on email body text (N = 93) for data collection, followed by both email header and URL (N = 75, N = 66, respectively).

10) **RQ10:** What are the trends across time in phishing email detection using NLP studies?

Figure 22 shows the distribution of phishing email detection studies in terms of publication year, indicating that studies have increased over the years. As can be observed, in the studies from 2006 to 2022, the highest number of publications rapidly grew from one publication in 2007 to an average of 12 studies in the last four years. It can also be noticed that the number of articles increased from six studies in 2012 and 2013. Moreover, there is a drop-down ratio of five publications in 2014 and 2015, and this has decreased to 4 in 2016 and 2017. There have been a total of 57 studies almost 57% of these 100 studies published during the period from 2018 to 2022. The highest number of studies was published in 2020, with 22 publications. The next highest publication year was 2018 and 2019, during which a total of 11 studies were published in phishing email detection using NLP techniques.

11) **RQ11:** What proportion of phishing email detection studies are on mixed language models?

Considering the outcomes of Figure 22 that show the distribution of phishing email detection studies in terms of publication year, the proportion of studies on mixed language models is 2%. Mostly, there are studies on English datasets for phishing email detection. There are two papers on Arabic phishing email detection using classical ML on mixed language models [112], [113]. Due to a lack of resources for Arabic spam/phishing emails, and the limited amount of progress achieved in tackling Arabic NLP in general, studies on Arabic phishing email detection are insufficient.

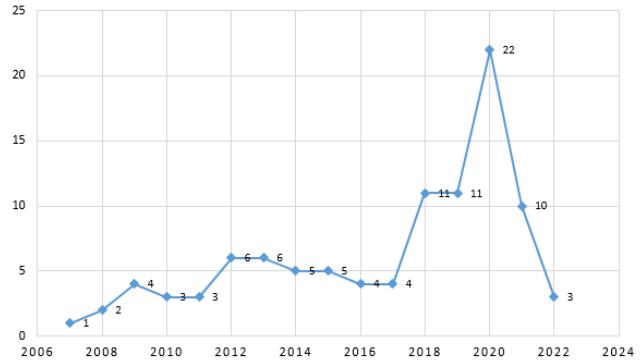

FIGURE 22. Distribution of phishing email detection studies per publication year.

V. DISCUSSION

This section presents a discussion of the results presented in the section above. Figure 14 shows the Bar chart indicating the use of supervised algorithms including NB and SVM. The employment of unsupervised and semi-supervised system is expected to bring a revolution in the world of phishing detection. Interestingly, every algorithm has its own areas of application from the advanced SVM algorithm to the basic Naïve Bayes algorithm. The core of Machine Learning based models may contain a single algorithm, or even multiple algorithms. Appendix Table A1 indicates that there are way more multi-algorithm-based frameworks than the single algorithm models. The future research is also required to investigate the hybrid systems in detail.

To enhance the performance of the classifiers, optimisation algorithms have been used in several studies: [47], [52], [57], [59], [68], [70], [102], [105], [115], [126], [127], and the most important of them is the bio-inspired computing (BIC) optimisation technique [185]. The attributes of self-correction and enhancement are inherent in Bioinspired computing (BIC) algorithms, along with a natural tendency to adjust according to the consistently changing environments. BIC is capable of offering flexible, efficient and multifaceted computational algorithms. BIC algorithms have been used in different fields in the past few years to solve issues. BIC solution can be obtained by selecting appropriate dimensions of the problem, assessing the significance of the comparative solutions and describing the operators. Research is being carried out on BIC processes to resolve complicated computational problems [186].

Figure 14 represents a bar chart that depicts that 80% of the considered research studies have formulated and benchmarked anti-phishing systems through the use of supervised techniques; thus, indicating higher inclination of researchers towards the use of supervised techniques. In short, Figure 14 implies the preference of the researchers and system developers to make use of supervised approaches which indicates extensive scope of conducting further research on semi-supervised, unsupervised and reinforcement based models in context of phishing [44]–[64], [66], [70], [77]–[82], [84]–[99], [101], [102], [105]–[112], [115]–[128], [131], [132], [153], [164], [196]–[198]. Experts interested in developing anti-phish systems based on Artificial Intelligence must understand that only unsupervised Machine learning can render the desired outcomes; hence, more research is required to get complete insight into unsupervised ML. A comparison of supervised and unsupervised ML techniques shows that the scope of the latter is broader than the former since non-supervised phishing detection frameworks can outperform the supervised ML-based counterparts if properly applied and exploited. This may be attributed to certain features of unsupervised learning that make it a better choice in comparison to supervised learning. These features include easier computations and easier accessibility to unlabeled data as compared to labeled data.

Figure 21 shows 91 studies that involved the use of ML algorithms during the development of phish detection systems. The data revealed that header or domain features (exclusive of subject field) were employed in just 29% of these studies (i.e. 27 studies). This indicates the need for more diligent analysis of e-mail with respect to header, domain and URL-based features. Moreover, only the set of selective features have been employed in the frameworks with no consideration to some essential features like 'Received from,' header fields, 'Age of domain' and others. Hence, it is imperative to consider using the overlooked header, URL and domain features in future in phish detection frameworks during the implementation of feature engineering for developing a competent feature set.

Usually, the word-based clustering or classification models are used in the studies investigating e-mail phish detection. The phish is detected on the basis of the similarity of the models and clusters with common phish words. Despite the logic behind these models and clusters, it is not easy to prevent phishing since the phishers have also become more robust and they tend to design their phishing content and emails with due consideration to all the security techniques and approaches and the psychology of internet users. Usually, the phishers design their phishing content by including words and phrases relevant to finance and other interesting subjects in the message body. They specifically tend to design the 'Subject' header in such a way that the users become compelled

to check the email and ultimately become the victim of phishing attack. This implies that phishing email detection through content analysis or normal word-based analysis can be made more effective by using automated mechanism for timely detection of phishing emails. The automated mechanism allows identifying the similarity between the email and the structure explained earlier in Figure 3. After checking for similarities, the automated mechanism tags the email as either phishing or legitimate. There is a dearth of recent studies on the use of such an automated mechanism while applying content based analysis techniques. Hence, future research must be performed to explore this undiscovered subject of content analysis (including subject header). This also suggests that an effective ML based framework for phishing detection must be competent enough to identify phisher and fraudsters despite all the mentioned challenges. The earlier research can serve as the guideline for researchers interested in exploring this domain in future.

The last decade showed considerable rise in the number of studies published annually; the stats indicated in Figure 22 shows that there was only one research article published in 2006 while the following ten years showed an average of 4 research articles on an annual basis. The growing interest of researchers in this domain is expected to result in emergence of better and novel techniques for phishing detection. Moreover, with the outbreak of the Corona pandemic in 2019 and 2020, the phishing attacks were on peak and hence, the years 2019 and 2020 depicted a significant rise in the number of research articles published in this domain. Since the month of September, the next year, a number of researchers started their studies on Phishing attacks in context of coronavirus disease (COVID-19). Generally, phishers use texts relevant to COID-19 pandemic or about internet technologies and security to attract their victims and conduct Phishing attacks [1]. The collected data revealed significant rise in the number of phishing attacks being made and a consequent elevation in the losses being caused by phishing activities. Appendix Table A1 indicates the inclination of the scholars towards the use of the popular NLP technique (e.g., Lexical analysis, POS, NER, tagging, language detection and identification of semantic relationships, Char-level email (header & body), word-level email (header & body) in context of phishing [49], [51], [63], [64], [78], [80]–[82], [89], [109].

One of the most popular databases that entail significant research works pertaining to phishing email detection is none other than Google Scholar depicted in Figure 10. Next in the line are databases like Springer, IEEE, ScienceDirect, ACM Digital Library, Wiley Online Library, SAGE Pub, Emerald, and Taylor and Francis Online databases. All the mentioned databases are highly known for entailing competent research works associated with phishing email detection. The researches included in the databases also shed light on various NLP techniques and their use with regards to phishing detection. These databases can prove helpful for scholars in extracting relevant studies about phishing e-mail detection while conducting research in future.

Specifically, including the feature selection techniques, the current paper provides critical investigations of the study regarding phishing email detection techniques. It also demonstrates the weak points linked to every included research. Moreover, it enlightens the ML classifiers, including their correlated features selection technique, which is stated in the research. The results of the included research study have been considered with regards to several factors, and these factors are the approval of redundant or independent features, value diverseness, feature hybridity, high dimensionality in data, imbalanced data and the performance outlined through the features for the detection of unfamiliar types of phishing attacks included in web data. Additionally, through implementing an extra feature, it will become feasible to assist the choice of most applicable feature/features as discovered from this review; this can effortlessly avoid the problem discussed earlier. However, a limited quantity of applicable redundant features can be implemented alongside the extra feature to detect phishing, which can consequently provide improved selection outcome. Thus, the possibility of imbalanced dataset selection is reduced in addition, with a fair decrease in dataset dimensionality. It is considered that when the classification is specific, operating duration is lesser, easier estimations can be made, with least storage and errors and false detection related cost being less as well, as these can allow a phishing detection to be effective. Therefore, it can be seen that the proposal of utilising an extra feature can be emphasised in future research, along with the advantages associated with these features at the time of detection of a hybrid phishing email.

To restrict the activity of phishers, it is crucial that at the time of performing research in the future, one should take into consideration the view of attackers or phishers in regards with the phishing issues, along with phishers' emotions and their aims. As stated by Haskin *et al.* [199] in his 2018 research that financial and intellectual features are amongst those several definite factors that might invigorate the phishers to indulge in phishing attacks.

NNs were seen as a good tool for detecting phishing attacks, however it can be a poor choice in terms of phishing detection due to the features of detailed training needs along with specific skills vital for parameter tuning. The ML techniques are also reckoned by the experts for detecting phishing attacks. Furthermore, failing to notice the phishing attacks developed via procedure such as squatting, tab-napping and malvertising, it was seen that the number of research studies carried out in the domain of avoiding phishing and detection procedures were usually on the subject found in the message of phishing e-mails. Nonetheless, to detect and resolve phishing emails appropriately, the research these days examine the production of the NLP technique, and by employing semantic change, the phishing can be observed via NLP. In addition, even though NLP is not tested on huge datasets as yet, as per the research, it is identified as having good precision in contrast with different techniques of detecting phishing emails [46]. When conducting research in the future, the

influence of the human aspect and phishing related education methods must be taken into consideration, as they have been neglected in the existing literature because of great emphasis on novel techniques and tools linked with phishing detection. The emphasis of researchers on non-semantic feature analysis till date, even though they are not related to identifying the sender's aim, must be rectified. The work is made more complex by selected phishing emails being falsified by the phishers for instance; spear-phishing or whaling by utilising personal information gathered from social networking sites (SNS). The detection system that relies on listing or malware analysis in regards to detecting the emails finds it difficult to work in areas without attachments or links. The need to extract the definition of the body content of an email is required at the time of beginning intention analysis. Furthermore, for the email content to be semantically prepared, the addition of semantic in the research is needed; this way, the detection aim can be obtained. An attentive research is required to be performed, so that it brings out indications and expressions from the email body text in order to control the phishing problems. A semantic analysis should be made of the email body text and the features, for instance, sentences and words, must be used to identify the legitimacy of the email.

Most of the procedures linked with the detection of phishing emails generally uses the ML techniques, specifically classification and clustering. Therefore, ML-based evaluation metrics and approaches are utilised by these techniques. The evaluation results can fall to disuse in the long-term, due to the constant developing character of phishers. Consequently, the complexity of the cybersecurity domain is increased. Nonetheless, this issue can be controlled if the evolving of evaluation results is given particular heed. The experts linked to phishing detection must attempt and devise adaptable evaluation plans that can be amended when needed to ensure cybersecurity. In this way, it will be easier to prevent the drawbacks such as inadequate time validity and range. Thus, in this respect, there are several classifications of the dataset that have been developed by researchers and specialists that depend on the type of the related dataset, and time and place, and only then can the research on every class of the dataset begin. The accurate contrast of several phishing detection techniques is hard to produce because of the lack of basic benchmarks. Moreover, this is high time for the researchers to constantly try and devise plans that can reduce the negative impact of the above-mentioned problems related to phishing detection techniques. This is because inconsiderate giving out of sensitive data along with evolution of phishers, result in the non-availability of reference datasets.

This systematic review is limited in the sense that it has only included research studies extracted from specific databases (like The ACM Digital Library, Emerald, Google Scholar, IEEE, ScienceDirect, Springer, Taylor and Francis Online, and Wiley Online Library). Consequently, there is probability that the included databases may fail to fully represent content entailed in missed studies relevant to the topic of phishing email detection and the subject of NLP Techniques used for phishing detection. It is possible to rectify this limitation in future research through the inclusion of databases like Web of Science, Scopus, ERIC, ProQuest that have not been considered in this study.

VI. CONCLUSION

Presently, one of the most interesting topics in the domain of cybersecurity is assumed to be phishing email detection. In this research, journal, conference, and workshop papers were carefully analysed, published between 2006 and 2022, with different techniques to investigate the trend of phishing email detection. A systematic literature review was employed to select 100 publications. All types of phishing email detection, for example, 'the domain name is misspelt,' 'the email is poorly written,' 'suspicious attachments or links' and 'phishing warning messages,' have been covered in our research. The background information regarding the phishing ecosystem is first presented along with the valuable phishing statistics. Next, the taxonomy of phishing detection schemes are then stated, and the phishing email detection datasets and phishing email detection features are discussed along with the detection algorithms and evaluation metrics. Lastly, recommendations are presented which can help with the phishing detection schemes' effective development, so that the compare-and-contrast schemes can be easily carried out.

This survey is unique in the sense that it relates work to their openly available tools and resources. The analysis of the presented work revealed that not much had been discussed about phishing email detection using NLP techniques. Therefore, many open issues are associated with this phishing email detection. An evolving research area is illustrated by this phishing email detection. However, all the presented resources are not publicly available so far. Various research questions arise with this survey: (1) Is manually built resource-effective, or is it better to suggest techniques to automatically produce such resources? (2) Why do the research studies always follow the way of construction? (3) Can we depend on the existing resources to combine resources, etc.? (4) Are deep learning approaches more helpful and time-saving as compared to conventional approaches such as NB, SVM, etc., for phishing email detection?

Considering the outcomes of the systematic literature review, it is observed that phishing email detection is considered as the main research field, and research community has tried hard to address this problem in various common languages like English. Yet, it hasn't been possible to generalize those findings to the rest of the cultures or environments like the developing non-English-speaking nations, where the Arab world is no exception. Arabic language is considered to be a Semitic language attributed with rich morphology. This aids in our motivation towards the problem of Arabic language phishing emails for the removal of language barriers. There are very few papers on Arabic spam/phishing email detection on classical machine learning [112]. Due to a lack of resources for Arabic spam/phishing emails and the

limited amount of progress achieved in tackling Arabic NLP in general, studies on Arabic phishing email detection are insufficient.

Offering the latest resources and tools to the community of research is the key idea of this survey. The overall objective is to present the strengths and weaknesses of each resource to the community. It is evident that after 2019, there has been a dramatic upsurge in the number of deep learning techniques adopted by researchers in the phishing email detection. The findings revealed that further work is required to employ modernised, deep learning techniques in phishing email detection studies; for instance, long-short-term memory (LSTM) and CNN models. The tools and resources are not sufficient in this research area. Hence, the researchers are in dire need to perform more research to assess deep learning techniques in the phishing email detection domain. The steady performance of the model was the reason for the great acceptance of supervised approaches, as various distinct observations – particularly in the field of machine learning-based proposal – were seen from the outcome of the study, after its detailed investigation. Moreover, as outlined, there are some algorithms which have significant requirements, for instance NB and SVM. Also, the bio-inspired computing (BIC) optimisation technique has been used in several studies and has significantly improved the performance of classifiers and reduced security challenges related to costs of misclassification as well as user-dependent costs of misclassification.

Summing up, we have seen that the most commonly utilised are single-algorithm anti-phish systems, for this reason the possibility of analysis into hybrid and multi-algorithm systems is fairly positive. Apart from the research which emphasises on email header features, except for the URLs in the email body, subject field and sender domain data must be greatly considered going forward. Furthermore, the presentation of 'Concept Drift' is an essential field that could contribute to improving methods for detecting phishing attacks. A fresh concept that is used is social honeypots and recommendation system algorithms, which are used for: detection of phishing that occurs between two malicious profiles and also for the detection of similar phishing emails. Through this method, the detection of phishing emails occurs more rapidly. However, there is a need for some innovative ideas that can consider each perspective of an issue, as the recent method has not proven as effective in regards to managing phishing emails nature. Even governments of many notable countries around the world, despite being reproached by several bodies have failed to produce an efficient procedure that has a long-term influence on this problem. Having said that, it is seen lately that a greater significance is given to invigorate cybersecurity' consequently, a rise in research and fair accessibility of funds in this area have also been observed. Therefore, it is anticipated that a tough framework, set up with actions opposed to the pitfalls outlined in this work can be made accessible for both individual and commercial implementations.

APPENDIX

Appendixes, if needed, appear in a separate file.

ACKNOWLEDGMENT

This work is a part of a thesis to be submitted in fulfilment of the Ph.D. degree with the School of Science, Engineering and Environment, University of Salford.

REFERENCES

[1] (2020). Anti-Phishing Working Group. *Phishing Activity Trends Report 3rd Quarter 2020.* [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q3_2020.pdf
[2] (2021). *Phishing Activity Trends Report 3rd Quarter 2021*. Anti-Phishing Working Group. [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q3_2021.pdf
[3] N. A. Khan, S. N. Brohi, and N. Zaman, "Ten deadly cyber security threats amid COVID-19 pandemic," TechRxiv, Tech. Rep., 2020, doi: 10.36227/techrxiv.12278792.v1.
[4] B. Pranggono and A. Arabo, "COVID-19 pandemic cybersecurity issues," *Internet Technol. Lett.*, vol. 4, no. 2, Mar. 2021, doi: 10.1002/itl2.247.
[5] H. Abroshan, J. Devos, G. Poels, and E. Laermans, "COVID-19 and phishing: Effects of human emotions, behavior, and demographics on the success of phishing attempts during the pandemic," *IEEE Access*, vol. 9, pp. 121916–121929, 2021, doi: 10.1109/ACCESS.2021.3109091.
[6] D. Irani, S. Webb, J. Giffin, and C. Pu, "Evolutionary study of phishing," in *Proc. eCrime Res. Summit*, Oct. 2008, pp. 1–10, doi: 10.1109/ECRIME.2008.4696967.
[7] B. Parno, C. Kuo, and A. Perrig, "Phoolproof phishing prevention," in *Proc. Int. Conf. Financial Cryptography Data Secur.*, 2006, pp. 1–19, doi: 10.1007/11889663_1.
[8] R. Verma, N. Shashidhar, and N. Hossain, "Detecting phishing emails the natural language way," in *Proc. Eur. Symp. Res. Comput. Secur.*, vol. 7459, 2012, pp. 824–841, doi: 10.1007/978-3-642-33167-1_47.
[9] Z. Dou, I. Khalil, A. Khreishah, A. Al-Fuqaha, and M. Guizani, "Systematization of knowledge (SoK): A systematic review of software-based web phishing detection," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2797–2819, 2017, doi: 10.1109/COMST.2017.2752087.
[10] A. Das, S. Baki, A. El Aassal, R. Verma, and A. Dunbar, "SoK: A comprehensive reexamination of phishing research from the security perspective," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 671–708, Dec. 2019, doi: 10.1109/COMST.2019.2957750.
[11] T. Sharma. (2021). *Evolving Phishing Email Prevention Techniques: A Survey to Pin Down Effective Phishing Study Design Concepts*. [Online]. Available: http://hdl.handle.net/2142/109179
[12] A. Mukherjee, N. Agarwal, and S. Gupta, "A survey on automatic phishing email detection using natural language processing techniques," *Int. Res. J. Eng. Technol.*, vol. 6, no. 11, pp. 1881–1886, 2019.
[13] A. Almomani, B. B. Gupta, S. Atawneh, A. Meulenberg, and E. Almomani, "A survey of phishing email filtering techniques," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 2070–2090, 4th Quart., 2013, doi: 10.1109/SURV.2013.030713.00020.
[14] S. Salloum, T. Gaber, S. Vadera, and K. Shaalan, "Phishing email detection using natural language processing techniques: A literature survey," *Proc. Comput. Sci.*, vol. 189, pp. 19–28, Jan. 2021, doi: 10.1016/j.procs.2021.05.077.
[15] A. Vadariya and N. K. Jadav, "A survey on phishing URL detection using artificial intelligence," in *Proc. Int. Conf. Recent Trends Mach. Learn., IoT, Smart Cities Appl.*, 2021, pp. 9–20, doi: 10.1007/978-981-15-7234-0_2.
[16] D. Sahoo, C. Liu, and S. C. H. Hoi, "Malicious URL detection using machine learning: A survey," 2017, *arXiv:1701.07179*.
[17] E. S. Aung, C. T. Zan, and H. Yamana, "A Survey of URL-based phishing detection," in *Proc. DEIM Forum*, 2019, pp. 2–3.
[18] C. M. R. D. Silva, E. L. Feitosa, and V. C. Garcia, "Heuristic-based strategy for phishing prediction: A survey of URL-based approach," *Comput. Secur.*, vol. 88, Jan. 2020, Art. no. 101613, doi: 10.1016/j.cose.2019.101613.
[19] V. V. Satane and A. Dasgupta, "Survey paper on phishing detection: Identification of malicious URL using Bayesian classification on social network sites," *Int. J. Sci. Res.*, vol. 4, no. 4, pp. 1998–2001, 2013.

[20] A. Aleroud and L. Zhou, "Phishing environments, techniques, and countermeasures: A survey," *Comput. Secur.*, vol. 68, pp. 160–196, Jul. 2017. 10.1016/j.cose.2017.04.006.

[21] R. M. Mohammad, F. Thabtah, and L. McCluskey, "Tutorial and critical analysis of phishing websites methods," *Comput. Sci. Rev.*, vol. 17, pp. 1–24, Aug. 2015, doi: 10.1016/j.cosrev.2015.04.001.

[22] G. Varshney, M. Misra, and P. K. Atrey, "A survey and classification of web phishing detection schemes," *Secur. Commun. Netw.*, vol. 9, no. 18, pp. 6266–6284, Dec. 2016, doi: 10.1002/sec.1674.

[23] L. Tang and Q. H. Mahmoud, "A survey of machine learning-based solutions for phishing website detection," *Mach. Learn. Knowl. Extraction*, vol. 3, no. 3, pp. 672–694, Aug. 2021, doi: 10.3390/make3030034.

[24] I. Qabajeh, F. Thabtah, and F. Chiclana, "A recent review of conventional vs. Automated cybersecurity anti-phishing techniques," *Comput. Sci. Rev.*, vol. 29, pp. 44–55, Aug. 2018, doi: 10.1016/j.cosrev.2018.05.003.

[25] M. Khonji, Y. Iraqi, and A. Jones, "Phishing detection: A literature survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 2091–2121, 4th Quart, 2013, doi: 10.1109/SURV.2013.032213.00009.

[26] B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, "Fighting against phishing attacks: State of the art and future challenges," *Neural Comput. Appl.*, vol. 28, no. 12, pp. 3629–3654, Dec. 2017, doi: 10.1007/s00521-016-2275-y.

[27] 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.*, vol. 67, no. 2, pp. 247–267, Feb. 2018, doi: 10.1007/s11235-017-0334-z.

[28] K. L. Chiew, K. S. C. Yong, and C. L. Tan, "A survey of phishing attacks: Their types, vectors and technical approaches," *Expert Syst. Appl.*, vol. 106, pp. 1–20, Sep. 2018, doi: 10.1016/j.eswa.2018.03.050.

[29] *PhishTank: An Anti-Phishing Site*. LLC OpenDNS, San Francisco, CA, USA. Accessed: Dec. 5, 2016. [Online]. Available: https://www.phishtank.com

[30] *APWG Phishing Trends Reports*, Anti Phishing Working Group, 2016.

[31] G. Xiang, J. Hong, C. P. Rose, and L. Cranor, "CANTINA+: A feature-rich machine learning framework for detecting phishing web sites," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 2, pp. 1–28, Sep. 2011, doi: 10.1145/2019599.2019606.

[32] G. Ramesh, I. Krishnamurthi, and K. S. S. Kumar, "An efficacious method for detecting phishing webpages through target domain identification," *Decis. Support Syst.*, vol. 61, pp. 12–22, May 2014, doi: 10.1016/j.dss.2014.01.002.

[33] C. Karlof, U. Shankar, J. D. Tygar, and D. Wagner, "Dynamic pharming attacks and locked same-origin policies for web browsers," in *Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS)*, 2007, pp. 58–71, doi: 10.1145/1315245.1315254.

[34] Z. Dou, "Secure entity authentication," Ph.D. dissertation, New Jersey Inst. Technol., Newark, NJ, USA, 2018.

[35] C. Whittaker, B. Ryner, and M. Nazif, "Large-scale automatic classification of phishing pages," Tech. Rep., 2010.

[36] E. E. Lastdrager, "Achieving a consensual definition of phishing based on a systematic review of the literature," *Crime Sci.*, vol. 3, no. 1, pp. 1–10, Dec. 2014, doi: 10.1186/s40163-014-0009-y.

[37] A. Emigh, "The crimeware landscape: Malware, phishing, identity theft and beyond," *J. Digit. Forensic Pract.*, vol. 1, no. 3, pp. 245–260, Sep. 2006, doi: 10.1080/15567280601049985.

[38] S. Abraham and I. Chengalur-Smith, "An overview of social engineering malware: Trends, tactics, and implications," *Technol. Soc.*, vol. 32, no. 3, pp. 183–196, 2010, doi: 10.1016/j.techsoc.2010.07.001.

[39] G. Park and J. Rayz, "Ontological detection of phishing emails," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2018, pp. 2858–2863, doi: 10.1109/SMC.2018.00486.

[40] (2020). University of Massachusetts Amherst. [Online]. Available: https://www.umass.edu/it/freshphish

[41] H. Kim and J. H. Huh, "Detecting DNS-poisoning-based phishing attacks from their network performance characteristics," *Electron. Lett.*, vol. 47, no. 11, pp. 656–658, May 2011.

[42] B. B. Gupta and Q. Z. Sheng, *Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices*. Boca Raton, FL, USA: CRC Press, 2019.

[43] E. Blanzieri and A. Bryl, "A survey of learning-based techniques of email spam filtering," *Artif. Intell. Rev.*, vol. 29, no. 1, pp. 63–92, 2008, doi: 10.1007/s10462-009-9109-6.

[44] 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, May 2020, doi: 10.11591/csit.v1i1.p1-12.

[45] R. Vinayakumar, K. P. Soman, P. Poornachandran, V. S. Mohan, and A. D. Kumar, "ScaleNet: Scalable and hybrid framework for cyber threat situational awareness based on DNS, URL, and email data analysis," *J. Cyber Secur. Mobil.*, vol. 8, no. 2, pp. 189–240, 2018, doi: 10.13052/jcsm2245-1439.823.

[46] A. Kumar, J. M. Chatterjee, and V. G. Díaz, "A novel hybrid approach of SVM combined with NLP and probabilistic neural network for email phishing," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 1, p. 486, Feb. 2020, doi: 10.11591/ijece.v10i1.pp486-493.

[47] W. Niu, X. Zhang, G. Yang, Z. Ma, and Z. Zhuo, "Phishing emails detection using CS-SVM," in *Proc. IEEE Int. Symp. Parallel Distrib. Process. Appl. IEEE Int. Conf. Ubiquitous Comput. Commun. (ISPA/IUCC)*, Dec. 2017, pp. 1054–1059, doi: 10.1109/ISPA/IUCC.2017.00160.

[48] M. Hamisu and A. Mansour, "Detecting advance fee fraud using NLP bag of word model," in *Proc. IEEE 2nd Int. Conf. Cyberspac (CYBER NIGERIA)*, Feb. 2021, pp. 94–97, doi: 10.1109/CYBERNIGERIA51635.2021.9428793.

[49] A. Junnarkar, S. Adhikari, J. Fagania, P. Chimurkar, and D. Karia, "E-mail spam classification via machine learning and natural language processing," in *Proc. 3rd Int. Conf. Intell. Commun. Technol. Virtual Mobile Netw. (ICICV)*, Feb. 2021, pp. 693–699, doi: 10.1109/ICICV50876.2021.9388530.

[50] M. S. Swetha and G. Sarraf, "Spam email and malware elimination employing various classification techniques," in *Proc. 4th Int. Conf. Recent Trends Electron., Inf., Commun. Technol. (RTEICT)*, May 2019, pp. 140–145, doi: 10.1109/RTEICT46194.2019.9016964.

[51] Y. Lee, J. Saxe, and R. Harang, "CATBERT: Context-aware tiny BERT for detecting social engineering emails," 2020, *arXiv:2010.03484*.

[52] R. Vinayakumar, K. P. Soman, P. Poornachandran, S. Akarsh, and M. Elhoseny, "Deep learning framework for cyber threat situational awareness based on email and URL data analysis," in *Cybersecurity and Secure Information Systems*. Berlin, Germany: Springer, 2019, pp. 87–124, doi: 10.1007/978-3-030-16837-7_6.

[53] G. Egozi and R. Verma, "Phishing email detection using robust NLP techniques," in *Proc. IEEE Int. Conf. Data Mining Workshops (ICDMW)*, Nov. 2018, pp. 7–12, doi: 10.1109/ICDMW.2018.00009.

[54] E. S. Gualberto, R. T. De Sousa, T. P. De Brito Vieira, J. P. C. L. Da Costa, and C. G. Duque, "The answer is in the text: Multi-stage methods for phishing detection based on feature engineering," *IEEE Access*, vol. 8, pp. 223529–223547, 2020, doi: 10.1109/ACCESS.2020.3043396.

[55] F. Janjua, A. Masood, H. Abbas, and I. Rashid, "Handling insider threat through supervised machine learning techniques," *Proc. Comput. Sci.*, vol. 177, pp. 64–71, Jan. 2020, doi: 10.1016/j.procs.2020.10.012.

[56] E. M. Bahgat, S. Rady, W. Gad, and I. F. Moawad, "Efficient email classification approach based on semantic methods," *Ain Shams Eng. J.*, vol. 9, no. 4, pp. 3259–3269, Dec. 2018, doi: 10.1016/j.asej.2018.06.001.

[57] M. U. Chowdhury, J. H. Abawajy, A. V. Kelarev, and T. Hochin, "Multi-layer hybrid strategy for phishing email zero-day filtering," *Concurrency Computation: Pract. Exper.*, vol. 29, no. 23, p. e3929, Dec. 2017, doi: 10.1002/cpe.3929.

[58] N. B. Harikrishnan, R. Vinayakumar, and K. P. Soman, "A machine learning approach towards phishing email detection," in *Proc. Anti-Phishing Pilot ACM Int. Workshop Secur. Privacy Analytics (IWSPA AP)*, 2018, pp. 455–468. [Online]. Available: http://ceur-ws.org/

[59] J. Zhang, W. Li, L. Gong, Z. Gu, and J. Wu, "Targeted malicious email detection using hypervisor-based dynamic analysis and ensemble learning," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6, doi: 10.1109/GLOBECOM38437.2019.9014069.

[60] X. Li, D. Zhang, and B. Wu, "Detection method of phishing email based on persuasion principle," in *Proc. IEEE 4th Inf. Technol., Netw., Electron. Autom. Control Conf. (ITNEC)*, Jun. 2020, pp. 571–574, doi: 10.1109/ITNEC48623.2020.9084766.

[61] J. Rastenis, S. Ramanauskaitė, I. Suzdalev, K. Tunaitytė, J. Janulevičius, and A. Čenys, "Multi-language spam/phishing classification by email body text: Toward automated security incident investigation," *Electronics*, vol. 10, no. 6, p. 668, 2021, doi: 10.3390/electronics10060668.

[62] V. D. Sharma, S. K. Yadav, S. K. Yadav, K. N. Singh, and S. Sharma, "An effective approach to protect social media account from spam mail—A machine learning approach," *Mater. Today, Proc.*, vol. 2021, pp. 1–7, Feb. 2021, doi: 10.1016/j.matpr.2020.12.377.

[63] E. Castillo, S. Dhaduvai, P. Liu, K.-S. Thakur, A. Dalton, and T. Strzalkowski, "Email threat detection using distinct neural network approaches," in *Proc. 1st Int. Workshop Social Threats Online Conversations, Understand. Manage.*, 2020, pp. 48–55. [Online]. Available: https://aclanthology.org/2020.stoc-1.8

[64] T. Peng, I. Harris, and Y. Sawa, "Detecting phishing attacks using natural language processing and machine learning," in *Proc. IEEE 12th Int. Conf. Semantic Comput. (ICSC)*, Jan. 2018, pp. 1210–1214, doi: 10.1109/ICCS45141.2019.9065490.

[65] N. A. Unnithan, N. B. Harikrishnan, R. Vinayakumar, K. P. Soman, and S. Sundarakrishna, "Detecting phishing E-mail using machine learning techniques," in *Proc. 1st Anti-Phishing Shared Task Pilot 4th ACM IWSPA Co-Located 8th ACM Conf. Data Appl. Secur. Privacy (CODASPY)*, 2018, pp. 51–54. [Online]. Available: http://ceur-ws.org

[66] U. Malaysia, "An enhanced online phishing e-mail detection framework based on evolving connectionist system," *Int. J. Innov. Comput., Inf. Control*, vol. 9, no. 3, pp. 1065–1086, 2013.

[67] R. Dazeley, J. L. Yearwood, B. H. Kang, and A. V. Kelarev, "Consensus clustering and supervised classification for profiling phishing emails in internet commerce security," in *Proc. Pacific Rim Knowl. Acquisition Workshop*, vol. 6232. Berlin, Germany: Springer, 2010, pp. 235–246, doi: 10.1007/978-3-642-15037-1_20.

[68] S. Seifollahi, A. Bagirov, R. Layton, and I. Gondal, "Optimization based clustering algorithms for authorship analysis of phishing emails," *Neural Process. Lett.*, vol. 46, no. 2, pp. 411–425, Oct. 2017, doi: 10.1007/s11063-017-9593-7.

[69] T. Stojnic, D. Vatsalan, and N. A. G. Arachchilage, "Phishing email strategies: Understanding cybercriminals' strategies of crafting phishing emails," *Secur. Privacy*, vol. 4, no. 5, p. e165, Sep. 2021, doi: 10.1002/spy2.165.

[70] R. Basnet, S. Mukkamala, and A. H. Sung, "Detection of phishing attacks: A machine learning approach," in *Soft Computing Applications in Industry* (Studies in Fuzziness and Soft Computing), vol. 226, B. Prasad, Eds. Berlin, Germany: Springer, 2008, doi: 10.1007/978-3-540-77465-5_19.

[71] P. R. K. Prosun, K. S. Alam, and S. Bhowmik, "Improved spam email filtering architecture using several feature extraction techniques," in *Proc. Int. Conf. Big Data, IoT, Mach. Learn.*, vol. 95, 2022, pp. 665–675, doi: 10.1007/978-981-16-6636-0_50.

[72] M. Manaswini and D. R. N. Srinivasu, "Phishing email detection model using improved recurrent convolutional neural networks and multilevel vectors," *Ann. Romanian Soc. Cell Biol.*, vol. 25, no. 6, pp. 16674–16681, 2021. [Online]. Available: http://annalsofrscb.ro

[73] J. Lee, F. Tang, P. Ye, F. Abbasi, P. Hay, and D. M. Divakaran, "D-fence: A flexible, efficient, and comprehensive phishing email detection system," in *Proc. IEEE Eur. Symp. Secur. Privacy (EuroS&P)*, Sep. 2021, pp. 578–597, doi: 10.1109/EuroSP51992.2021.00045.

[74] M. Hiransha, N. A. Unnithan, R. Vinayakumar, K. Soman, and A. D. R. Verma, "Deep learning based phishing e-mail detection," in *Proc. 1st AntiPhishing Shared Pilot 4th ACM Int. Workshop Secur. Privacy Anal. (IWSPA)*, 2018, pp. 1–5. [Online]. Available: http://ceur-ws.org

[75] R. Alotaibi, I. Al-Turaiki, and F. Alakeel, "Mitigating email phishing attacks using convolutional neural networks," in *Proc. 3rd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, Mar. 2020, pp. 1–6, doi: 10.1109/ICCAIS48893.2020.9096821.

[76] W. Pan, J. Li, L. Gao, L. Yue, Y. Yang, L. Deng, and C. Deng, "Semantic graph neural network: A conversion from spam email classification to graph classification," *Sci. Program.*, vol. 2022, pp. 1–8, Jan. 2022, doi: 10.1155/2022/6737080.

[77] I. AbdulNabi and Q. Yaseen, "Spam email detection using deep learning techniques," *Proc. Comput. Sci.*, vol. 184, pp. 853–858, Jan. 2021, doi: 10.1016/j.procs.2021.03.107.

[78] C. Thapa, J. W. Tang, A. Abuadbba, Y. Gao, S. Camtepe, S. Nepal, M. Almashor, and Y. Zheng, "Evaluation of federated learning in phishing email detection," 2020, *arXiv:2007.13300*.

[79] L. Halgaš, I. Agrafiotis, and J. R. C. Nurse, "Catching the Phish: Detecting phishing attacks using recurrent neural networks (RNNs)," in *Proc. Int. Workshop Inf. Secur. Appl.*, vol. 11897, Cham, Switzerland: Springer, 2019, pp. 219–233, doi: 10.1007/978-3-030-39303-8_17.

[80] A. Baccouche, S. Ahmed, D. Sierra-Sosa, and A. Elmaghraby, "Malicious text identification: Deep learning from public comments and emails," *Information*, vol. 11, no. 6, p. 312, Jun. 2020, doi: 10.3390/info11060312.

[81] 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, doi: 10.1109/ACCESS.2019.2913705.

[82] D. Xiao and M. Jiang, "Malicious mail filtering and tracing system based on KNN and improved LSTM algorithm," in *Proc. IEEE Int. Conf. Dependable, Autonomic Secure Comput., Int. Conf. Pervasive Intell. Comput., Int. Conf. Cloud Big Data Comput., Int. Conf. Cyber Sci. Technol. Congr. (DASC/PiCom/CBDCom/CyberSciTech)*, Aug. 2020, pp. 222–229.

[83] M. Crawford, T. M. Khoshgoftaar, J. D. Prusa, A. N. Richter, and H. A. Najada, "Survey of review spam detection using machine learning techniques," *J. Big Data*, vol. 2, no. 1, p. 23, 2015, doi: 10.1186/s40537-015-0029-9.

[84] A. A. Akinyelu and A. O. Adewumi, "Classification of phishing email using random forest machine learning technique," *J. Appl. Math.*, vol. 2014, pp. 1–6, Apr. 2014, doi: 10.1155/2014/425731.

[85] I. R. A. Hamid and J. H. Abawajy, "Profiling phishing email based on clustering approach," in *Proc. 12th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jul. 2013, pp. 628–635, doi: 10.1109/TrustCom.2013.76.

[86] I. R. A. Hamid and J. Abawajy, "Phishing email feature selection approach," in *Proc. IEEE 10th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Nov. 2011, pp. 916–921, doi: 10.1109/TrustCom.2011.126.

[87] A. Yasin and A. Abuhasan, "An intelligent classification model for phishing email detection," 2016, *arXiv:1608.02196*.

[88] W. N. Gansterer and D. Pölz, "E-mail classification for phishing defense," in *Proc. Eur. Conf. Inf. Retr.*, vol. 5478. Berlin, Germany: Springer, 2009, pp. 449–460, doi: 10.1007/978-3-642-00958-7_40.

[89] L. F. Gutiérrez, F. Abri, M. Armstrong, A. S. Namin, and K. S. Jones, "Phishing detection through email embeddings," 2020, *arXiv:2012.14488*.

[90] V. Listšk, Š. Let, J. Šedivý, and V. Hlavác, "Phishing email detection based on named entity recognition," in *Proc. 5th Int. Conf. Inf. Syst. Secur. Privacy (ICISSP)*, 2019, pp. 252–256.

[91] L. Ma, B. Ofoghi, P. Watters, and S. Brown, "Detecting phishing emails using hybrid features," in *Proc. Symp. Workshops Ubiquitous, Autonomic Trusted Comput.*, 2009, pp. 493–497, doi: 10.1109/UIC-ATC.2009.103.

[92] S. Smadi, N. Aslam, L. Zhang, R. Alasem, and M. A. Hossain, "Detection of phishing emails using data mining algorithms," in *Proc. 9th Int. Conf. Softw., Knowl., Inf. Manage. Appl. (SKIMA)*, Dec. 2015, pp. 1–8, doi: 10.1109/SKIMA.2015.7399985.

[93] G. Sonowal, "A model for detecting sounds-alike phishing email contents for persons with visual impairments," in *Proc. 6th Int. Conf. e-Learn. (econf)*, Dec. 2020, pp. 17–21, doi: 10.1109/econf51404.2020.9385451.

[94] V. S. Vinitha and D. K. Renuka, "Performance analysis of e-mail spam classification using different machine learning techniques," in *Proc. Int. Conf. Adv. Comput. Commun. Eng. (ICACCE)*, Apr. 2019, pp. 1–5, doi: 10.1109/ICACCE46606.2019.9080000.

[95] G. Yu, W. Fan, W. Huang, and J. An, "An explainable method of phishing emails generation and its application in machine learning," in *Proc. IEEE 4th Inf. Technol., Netw., Electron. Autom. Control Conf. (ITNEC)*, Jun. 2020, pp. 1279–1283, doi: 10.1109/ITNEC48623.2020.9085171.

[96] E. Markova, T. Bajtos, P. Sokol, and T. Mezesova, "Classification of malicious emails," in *Proc. IEEE 15th Int. Sci. Conf. Informat.*, vol. 231. Cham, Switzerland: Springer, Nov. 2019, pp. 279–284, doi: 10.1109/informatics47936.2019.9119329.

[97] R. Amin, M. M. Rahman, and N. Hossain, "A Bangla spam email detection and datasets creation approach based on machine learning algorithms," in *Proc. 3rd Int. Conf. Electr., Comput. Telecommun. Eng. (ICECTE)*, Dec. 2019, pp. 169–172, doi: 10.1109/ICECTE48615.2019.9303525.

[98] Y. Cohen, D. Hendler, and A. Rubin, "Detection of malicious webmail attachments based on propagation patterns," *Knowl.-Based Syst.*, vol. 141, pp. 67–79, Feb. 2018, doi: 10.1016/j.knosys.2017.11.011.

[99] S. Maldonado and G. L'Huillier, "SVM-based feature selection and classification for email filtering," in *Pattern Recognition-Applications Methods*, vol. 204. Berlin, Germany: Springer, 2013, pp. 135–148, doi: 10.1007/978-3-642-36530-0_11.

[100] M. A. Mohammed, S. S. Gunasekaran, S. A. Mostafa, A. Mustafa, and M. K. A. Ghani, "Implementing an agent-based multi-natural language anti-spam model," in *Proc. Int. Symp. Agent, Multi-Agent Syst. Robot. (ISAMSR)*, Aug. 2018, pp. 1–5, doi: 10.1109/ISAMSR.2018.8540555.

[101] A. Vazhayil, N. B. Harikrishnan, R. Vinayakumar, K. P. Soman, and A. D. R. Verma, "PED-ML: Phishing email detection using classical machine learning techniques," in *Proc. 1st AntiPhishing Shared Pilot 4th ACM Int. Workshop Secur. Privacy Anal. (IWSPA)*, 2018, pp. 1–8. [Online]. Available: http://ceur-ws.org

[102] S. Gibson, B. Issac, L. Zhang, and S. M. Jacob, "Detecting spam email with machine learning optimized with bio-inspired Metaheuristic algorithms," *IEEE Access*, vol. 8, pp. 187914–187932, 2020, doi: 10.1109/ACCESS.2020.3030751.

[103] L. Breiman, "Random forests," *Mach. Learn.*, vol. 45, no. 1, pp. 5–32, 2001.

[104] T. M. Mitchell, "Machine learning," Dept. Comput. Sci., Univ. Iasi, Romania, Tech. Rep., 1997.

[105] M. Arshey and A. V. K. S., "An optimization-based deep belief network for the detection of phishing e-mails," *Data Technol. Appl.*, vol. 54, no. 4, pp. 529–549, Jul. 2020, doi: 10.1108/DTA-02-2020-0043.

[106] S. Sankhwar, D. Pandey, and R. A. Khan, "Email phishing: An enhanced classification model to detect malicious URLs," *ICST Trans. Scalable Inf. Syst.*, vol. 6, no. 21, Jun. 2019, Art. no. 158529, doi: 10.4108/eai.13-7-2018.158529.

[107] F. Toolan and J. Carthy, "Phishing detection using classifier ensembles," in *Proc. eCrime Res. Summit*, Oct. 2009, pp. 1–9, doi: 10.1109/ECRIME.2009.5342607.

[108] R. Islam and J. Abawajy, "A multi-tier phishing detection and filtering approach," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 324–335, Jan. 2013, doi: 10.1016/j.jnca.2012.05.009.

[109] L. F. Gutierrez, F. Abri, M. Armstrong, A. S. Namin, and K. S. Jones, "Email embeddings for phishing detection," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2020, pp. 2087–2092, doi: 10.1109/BigData50022.2020.9377821.

[110] S. K. Sonbhadra, S. Agarwal, M. Syafrullah, and K. Adiyarta, "Email classification via intention-based segmentation," in *Proc. 7th Int. Conf. Electr. Eng., Comput. Sci. Informat. (EECSI)*, Oct. 2020, pp. 38–44, doi: 10.23919/EECSI50503.2020.9251306.

[111] E.-S.-M. El-Alfy and R. E. Abdel-Aal, "Using GMDH-based networks for improved spam detection and email feature analysis," *Appl. Soft Comput.*, vol. 11, no. 1, pp. 477–488, Jan. 2011, doi: 10.1016/j.asoc.2009.12.007.

[112] A. M. El-Halees, "Filtering spam e-mail from mixed Arabic and English messages: A comparison of machine learning techniques," *Int. Arab J. Inf. Technol.*, vol. 6, no. 1, pp. 1–14, 2009. [Online]. Available: http://hdl.handle.net/20.500.12358/25190.

[113] M. A. Mohammed, D. A. Ibrahim, and A. O. Salman, "Adaptive intelligent learning approach based on visual anti-spam email model for multi-natural language," *J. Intell. Syst.*, vol. 30, no. 1, pp. 774–792, Jun. 2021, doi: 10.1515/jisys-2021-0045.

[114] M. Sethi, S. Chandra, V. Chaudhary, and Y. Dahiya, "Spam email detection using machine learning and neural networks," in *Sentimental Analysis and Deep Learning*, vol. 1408. Singapore: Springer, 2022, pp. 275–290, doi: 10.1007/978-981-16-5157-1_22.

[115] G. Stringhini and O. Thonnard, "That ain't you: Blocking spearphishing through behavioral modelling," in *Proc. Int. Conf. Detection Intrusions Malware, Vulnerability Assessment*, vol. 9148. Cham, Switzerland: Springer, 2015, pp. 78–97, doi: 10.1007/978-3-319-20550-2_5.

[116] S. Duman, K. Kalkan-Cakmakci, M. Egele, W. Robertson, and E. Kirda, "EmailProfiler: Spearphishing filtering with header and stylometric features of emails," in *Proc. IEEE 40th Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Jun. 2016, pp. 408–416, doi: 10.1109/COMPSAC.2016.105.

[117] A. Bergholz, J. H. Chang, G. Paass, F. Reichartz, and S. Strobel, "Improved phishing detection using model-based features," in *Proc. CEAS*, 2008, pp. 1–10.

[118] I. Fette, N. Sadeh, and A. Tomasic, "Learning to detect phishing emails," in *Proc. 16th Int. Conf. World Wide Web (WWW)*, 2007, pp. 649–656, doi: 10.1145/1242572.1242660.

[119] S. R. Mirhoseini, F. Vahedi, and J. A. Nasiri, "E-mail phishing detection using natural language processing and machine learning techniques," Iran, Tech. Rep.

[120] C. E. Shyni, S. Sarju, and S. Swamynathan, "A multi-classifier based prediction model for phishing emails detection using topic modelling, named entity recognition and image processing," *Circuits Syst.*, vol. 7, no. 9, p. 2507, 2016, doi: 10.4236/cs.2016.79217.

[121] R. B. Basnet and A. H. Sung, "Classifying phishing emails using confidence-weighted linear classifiers," in *Proc. Int. Conf. Inf. Secur. Artif. Intell. (ISAI)*, 2010, pp. 108–112.

[122] F. Sanchez and Z. Duan, "A sender-centric approach to detecting phishing emails," in *Proc. Int. Conf. Cyber Secur.*, Dec. 2012, pp. 32–39, doi: 10.1109/CyberSecurity.2012.11.

[123] L. M. Stuart, G. Park, J. M. Talor, and V. Raskin, "On identifying phishing emails: Uncertainty in machine and human judgment," in *Proc. IEEE Conf. Norbert Wiener 21st Century (CW)*, Jun. 2014, pp. 1–8, doi: 10.1109/NORBERT.2014.6893870.

[124] G. Park, L. M. Stuart, J. M. Taylor, and V. Raskin, "Comparing machine and human ability to detect phishing emails," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2014, pp. 2322–2327, doi: 10.1109/SMC.2014.6974273.

[125] L. M. Form, K. L. Chiew, S. N. Sze, and W. K. Tiong, "Phishing email detection technique by using hybrid features," in *Proc. 9th Int. Conf. IT Asia (CITA)*, Aug. 2015, pp. 1–5, doi: 10.1109/CITA.2015.7349818.

[126] 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, Jun. 2016, doi: 10.1108/K-07-2014-0129.

[127] J. Abawajy and A. Kelarev, "A multi-tier ensemble construction of classifiers for phishing email detection and filtering," in *Proc. Int. Symp. Cyberspace Saf. Secur.*, vol. 7672. Berlin, Germany: Springer, 2012, pp. 48–56, doi: 10.1007/978-3-642-35362-8_5.

[128] J. Yearwood, M. Mammadov, and D. Webb, "Profiling phishing activity based on hyperlinks extracted from phishing emails," *Social Netw. Anal. Mining*, vol. 2, no. 1, pp. 5–16, Mar. 2012, doi: 10.1007/s13278-011-0031-y.

[129] S. Abu-Nimeh, D. Nappa, X. Wang, and S. Nair, "A distributed architecture for phishing detection using Bayesian additive regression trees," in *Proc. eCrime Researchers Summit*, Oct. 2008, pp. 1–10, doi: 10.1109/ECRIME.2008.4696965.

[130] J. P. M. De Sa, *Pattern Recognition: Concepts, Methods, and Applications*. Berlin, Germany: Springer, 2001.

[131] N. Moradpoor, B. Clavie, and B. Buchanan, "Employing machine learning techniques for detection and classification of phishing emails," in *Proc. Comput. Conf.*, Jul. 2017, pp. 149–156, doi: 10.1109/SAI.2017.8252096.

[132] E. M. Rudd, R. Harang, and J. Saxe, "MEADE: Towards a malicious email attachment detection engine," in *Proc. IEEE Int. Symp. Technol. Homeland Secur. (HST)*, Oct. 2018, pp. 1–7, doi: 10.1109/THS.2018.8574202.

[133] T. Gangavarapu and C. D. Jaidhar, "A novel bio-inspired hybrid meta-heuristic for unsolicited bulk email detection," in *Proc. Int. Conf. Comput. Sci.*, vol. 12139. Cham, Switzerland: Springer, 2020, pp. 240–254, doi: 10.1007/978-3-030-50420-5_18.

[134] M. N. Al-Mhiqani, R. Ahmad, Z. Z. Abidin, K. H. Abdulkareem, M. A. Mohammed, D. Gupta, and K. Shankar, "A new intelligent multilayer framework for insider threat detection," *Comput. Electr. Eng.*, vol. 97, Jan. 2022, Art. no. 107597, doi: 10.1016/j.compeleceng.2021.107597.

[135] A. Voulodimos, N. Doulamis, A. Doulamis, and E. Protopapadakis, "Deep learning for computer vision: A brief review," *Comput. Intell. Neurosci.*, vol. 2018, pp. 1–13, Feb. 2018, doi: 10.1155/2018/7068349.

[136] M. Hassaballah and A. I. Awad, *Deep Learning in Computer Vision: Principles and Applications*. Boca Raton, FL, USA: CRC Press, 2020.

[137] S. M. S. Islam, S. Rahman, M. M. Rahman, E. K. Dey, and M. Shoyaib, "Application of deep learning to computer vision: A comprehensive study," in *Proc. 5th Int. Conf. Informat., Electron. Vis. (ICIEV)*, May 2016, pp. 592–597, doi: 10.1109/ICIEV.2016.7760071.

[138] Y. Ning, S. He, Z. Wu, C. Xing, and L.-J. Zhang, "A review of deep learning based speech synthesis," *Appl. Sci.*, vol. 9, no. 19, p. 4050, Sep. 2019, doi: 10.3390/app9194050.

[139] H. Zen, "Deep learning in speech synthesis," in *Proc. 8th ISCA Speech Synth. Workshop*, Barcelona, Spain, 2013.

[140] A. B. Nassif, I. Shahin, I. Attili, M. Azzeh, and K. Shaalan, "Speech recognition using deep neural networks: A systematic review," *IEEE Access*, vol. 7, pp. 19143–19165, 2019, doi: 10.1109/ACCESS.2019.2896880.

[141] K. Noda, Y. Yamaguchi, K. Nakadai, H. G. Okuno, and T. Ogata, "Audio-visual speech recognition using deep learning," *Appl. Intell.*, vol. 42, no. 4, pp. 722–737, 2015, doi: 10.1007/s10489-014-0629-7.

[142] R. H. Abiyev, M. Arslan, and J. B. Idoko, "Sign language translation using deep convolutional neural networks," *KSII Trans. Internet Inf. Syst.*, vol. 14, no. 2, pp. 631–653, 2020, doi: 10.3837/tiis.2020.02.009.
[143] A. Pumsirirat and L. Yan, "Credit card fraud detection using deep learning based on auto-encoder and restricted Boltzmann machine," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 1, pp. 18–25, 2018. [Online]. Available: http://www.ijacsa.thesai.org/
[144] X. Zhang, Y. Han, W. Xu, and Q. Wang, "HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture," *Inf. Sci.*, vol. 557, pp. 302–316, May 2021, doi: 10.1016/j.ins.2019.05.023.
[145] X. Zhang, J. Zhao, and Y. LeCun, "Character-level convolutional networks for text classification," 2015, *arXiv:1509.01626*.
[146] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, 1997, doi: 10.1162/neco.1997.9.8.1735.
[147] C. Wartena and R. Brussee, "Topic detection by clustering keywords," in *Proc. 19th Int. Conf. Database Expert Syst. Appl.*, Sep. 2008, pp. 54–58, doi: 10.1109/DEXA.2008.120.
[148] M. Ruiz-Casado, E. Alfonseca, and P. Castells, "Automatic assignment of Wikipedia encyclopedic entries to WordNet synsets," in *Proc. Int. Atlantic Web Intell. Conf.*, vol. 3528, Berlin, Germany: Springer, 2005, pp. 380–386, doi: 10.1007/11495772_59.
[149] R. M. Esteves and C. Rong, "Using mahout for clustering Wikipedia's latest articles: A comparison between K-means and fuzzy C-means in the cloud," in *Proc. IEEE 3rd Int. Conf. Cloud Comput. Technol. Sci.*, Nov. 2011, pp. 565–569, doi: 10.1109/CloudCom.2011.86.
[150] B. Ghojogh, M. N. Samad, S. A. Mashhadi, T. Kapoor, W. Ali, F. Karray, and M. Crowley, "Feature selection and feature extraction in pattern analysis: A literature review," 2019, *arXiv:1905.02845*.
[151] E. Alpaydin, *Introduction to Machine Learning*, 3rd ed. Cambridge, MA, USA: MIT Press, 2014.
[152] C. M. Bishop, "Pattern recognition," *Mach. Learn.*, vol. 128, no. 9, 2006.
[153] M. Zareapoor and K. R. Seeja, "Feature extraction or feature selection for text classification: A case study on phishing email detection," *Int. J. Inf. Eng. Electron. Bus.*, vol. 7, no. 2, p. 60, 2015, doi: 10.5815/ijieeb.2015.02.08.
[154] M. A. Hall and L. A. Smith, "Practical feature subset selection for machine learning," in *Proc. 21st Australas. Comput. Sci. Conf. (ACSC)*, C. McDonald, Ed. Berlin, Germany: Springer, 1998, pp. 181–191. [Online]. Available: https://hdl.handle.net/10289/1512.
[155] S. Siddiqui, M. A. Rehman, S. M. Doudpota, and A. Waqas, "Ontology driven feature engineering for opinion mining," *IEEE Access*, vol. 7, pp. 67392–67401, 2019, doi: 10.1109/ACCESS.2019.2918584.
[156] T. Mori, "Information gain ratio as term weight: The case of summarization of ir results," in *Proc. 19th Int. Conf. Comput. Linguistics (COLING)*, 2002, pp. 1–7.
[157] G. Van Rossum and F. L. Drake, *Python Tutorial*, vol. 620. Amsterdam, The Netherlands: Centrum Voor Wiskunde en Informatica, 1995.
[158] F. Eibe, M. A. Hall, and I. H. Witten, *Data Mining: Practical Machine Learning Tools and Techniques*. San Mateo, CA, USA: Morgan Kaufmann, 2016.
[159] *TensorFlow Core | Machine Learning for Beginners and Experts*, 2019.
[160] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, and J. Vanderplas, "Scikit-learn: Machine learning in Python," *J. Mach. Learn. Res.*, vol. 12, pp. 2825–2830, Nov. 2011.
[161] E. Loper and S. Bird, "NLTK: The natural language toolkit," 2002, *arXiv: cs/0205028*.
[162] *MATLAB*, MathWorks, Natick, MA, USA, 2012.
[163] C. Sammut and G. I. Webb, *Encyclopedia of Machine Learning and Data Mining*. Berlin, Germany: Springer, 2017.
[164] V. Ramanathan and H. Wechsler, "Phishing detection and impersonated entity discovery using conditional random field and latent Dirichlet allocation," *Comput. Secur.*, vol. 34, pp. 123–139, May 2013, doi: 10.1016/j.cose.2012.12.002.
[165] M. Bekkar, H. K. Djemaa, and T. A. Alitouche, "Evaluation measures for models assessment over imbalanced data sets," *J. Inf. Eng. Appl.*, vol. 3, no. 10, pp. 1–13, 2013.
[166] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, "Learning to detect malicious URLs," *ACM Trans. Intell. Syst. Technol.*, vol. 2, no. 3, pp. 1–24, 2011, doi: 10.1145/1961189.1961202.
[167] R. B. Basnet and T. Doleck, "Towards developing a tool to detect phishing URLs: A machine learning approach," in *Proc. IEEE Int. Conf. Comput. Intell. Commun. Technol.*, Feb. 2015, pp. 220–223, doi: 10.1109/CICT.2015.63.
[168] P. Dewan and P. Kumaraguru, "Facebook inspector (FbI): Towards automatic real-time detection of malicious content on Facebook," *Social Netw. Anal. Mining*, vol. 7, no. 1, p. 15, 2017, doi: 10.1007/s13278-017-0434-5.
[169] H. Sha, Z. Zhou, Q. Liu, T. Liu, and C. Zheng, "Limited dictionary builder: An approach to select representative tokens for malicious URLs detection," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 7077–7082, doi: 10.1109/ICC.2015.7249455.
[170] *Anti-Phishing Working Group Phishing Archive*, APWG, 2014.
[171] R. Dhamija and J. D. Tygar, "The battle against phishing: Dynamic security skins," in *Proc. Symp. Usable Privacy Secur. (SOUPS)*, 2005, pp. 77–88, doi: 10.1145/1073001.1073009.
[172] M. Aburrous, M. A. Hossain, K. Dahal, and F. Thabtah, "Predicting phishing websites using classification mining techniques with experimental case studies," in *Proc. 7th Int. Conf. Inf. Technol., New Generat.*, 2010, pp. 176–181, doi: 10.1109/ITNG.2010.117.
[173] *PhishTank Phishing Archive*, 2014.
[174] *Apache Software Foundation (2014) Spamassassin Public Corpus*, 2006.
[175] M. Khonji, Y. Iraqi, and A. Jones, "Lexical URL analysis for discriminating phishing and legitimate websites," in *Proc. 8th Annu. Collaboration, Electron. Messaging, Anti-Abuse Spam Conf. (CEAS)*, 2011, pp. 422–427. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6148476
[176] *Enron Email Dataset*, Cohen, 2014.
[177] *AEUB Natural Language Processing Group*, T. E. S. Datasets, Athens, Greece., 2014.
[178] B. Klimt and Y. Yang, "The enron corpus: A new dataset for email classification research," in *Proc. Eur. Conf. Mach. Learn.*, vol. 3201. Berlin, Germany: Springer, 2004, pp. 217–226, doi: 10.1007/978-3-540-30115-8_22.
[179] K. Georgala, A. Kosmopoulos, and G. Paliouras, "Spam filtering: An active learning approach using incremental clustering," in *Proc. 4th Int. Conf. Web Intell., Mining Semantics (WIMS)*, 2014, pp. 1–12, doi: 10.1145/2611040.2611059.
[180] G. V. Cormack and T. R. Lynam, "TREC 2005 spam track overview," in *Proc. TREC*, 2005, pp. 274–500.
[181] *IronPort Anti-Spam*, 2014.
[182] T. Moore, R. Clayton, and H. Stern, "Temporal correlations between spam and phishing websites," in *Proc. LEET*, 2009, pp. 1–8.
[183] *SpamCopWiki: SpamTrap*, Jul. 2006.
[184] *The Phishload Phishing Test Database*.
[185] J. Batra, R. Jain, V. A. Tikkiwal, and A. Chakraborty, "A comprehensive study of spam detection in e-mails using bio-inspired optimization techniques," *Int. J. Inf. Manage. Data Insights*, vol. 1, no. 1, Apr. 2021, Art. no. 100006, doi: 10.1016/j.jjimei.2020.100006.
[186] M. K. Hanif, R. Talib, M. Awais, M. Y. Saeed, and U. Sarwar, "Comparison of bioinspired computation and optimization techniques," *Current Sci.*, vol. 115, no. 3, p. 450, Aug. 2018. [Online]. Available: https://www.jstor.org/stable/26978229.
[187] A. A. Sekh, D. P. Dogra, S. Kar, P. P. Roy, and D. K. Prasad, "ELM-HTM guided bio-inspired unsupervised learning for anomalous trajectory classification," *Cognit. Syst. Res.*, vol. 63, pp. 30–41, Oct. 2020, doi: 10.1016/j.cogsys.2020.04.003.
[188] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," Tech. Rep., 2007.
[189] D. Moher, A. Liberati, J. Tetzlaff, D. G. Altman, and G. Prisma, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *Ann. Internal Med.*, vol. 151, no. 4, pp. 264–269, 2009, doi: 10.7326/0003-4819-151-4-200908180-00135.
[190] V. Costa and S. Monteiro, "Knowledge processes, absorptive capacity and innovation: A mediation analysis," *Knowl. Process Manage.*, vol. 23, no. 3, pp. 207–218, Jul. 2016, doi: 10.1002/kpm.1507.
[191] D. Moher, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *Ann. Internal Med.*, vol. 151, no. 4, p. 264, Aug. 2009, doi: 10.7326/0003-4819-151-4-200908180-00135.
[192] M. Al-Emran, V. Mezhuyev, A. Kamaludin, and K. Shaalan, "The impact of knowledge management processes on information systems: A systematic review," *Int. J. Inf. Manage.*, vol. 43, pp. 173–187, Dec. 2018, doi: 10.1016/j.ijinfomgt.2018.08.001.

[193] S. Kitchenham and B. Charters, "Guidelines for performing systematic literature reviews in software engineering," Softw. Eng. Group, Sch. Comput. Sci. Math. Keele Univ., Keele, U.K., Tech. Rep., 2007.
[194] *Python*. [Online]. Available: https://www.python.org/
[195] *Weka*. [Online]. Available: https://www.cs.waikato.ac.nz/ml/weka/
[196] V. Ramanathan and H. Wechsler, "PhishGILLNET—Phishing detection methodology using probabilistic latent semantic analysis, AdaBoost, and co-training," *EURASIP J. Inf. Secur.*, vol. 2012, no. 1, pp. 1–22, Dec. 2012, doi: 10.1186/1687-417X-2012-1.
[197] I. R. A. Hamid and J. Abawajy, "Hybrid feature selection for phishing email detection," in *Proc. Int. Conf. Algorithms Architectures Parallel Process.*, vol. 7017. Berlin, Germany: Springer, 2011, pp. 266–275, doi: 10.1007/978-3-642-24669-2_26.
[198] F. Toolan and J. Carthy, "Feature selection for spam and phishing detection," in *Proc. eCrime Res. Summit*, Oct. 2010, pp. 1–12, doi: 10.1109/ecrime.2010.5706696.
[199] K. Hausken, "A cost–benefit analysis of terrorist attacks," *Defence Peace Econ.*, vol. 29, no. 2, pp. 111–129, Feb. 2018, doi: 10.1080/10242694.2016.1158440.

SAID SALLOUM received the bachelor's degree in computer science from Yarmouk University and the M.Sc. degree (Hons.) in informatics (knowledge and data management) from The British University in Dubai. He recently worked with the University of Sharjah's Research Institute of Sciences and Engineering (RISE) on a variety of research topics. Since 2013, he has been an Oracle Expert and holds multiple oracle certifications. He is among the top 2% of scientists in the world, according to the report published by Stanford University, in October 2021. Also, according to AD Scientific Index 2022, he was chosen as the best 100 scientists in United Arab Emirates. His majority of publications were indexed in ISI Web of Science.

TAREK GABER received the Ph.D. degree in computer science from The University of Manchester, Manchester, U.K., in 2012. He has worked in many universities including the Faculty of Computers and Informatics, Suez Canal University; the Faculty of Computers and Information Sciences, Ain Shams University; and the School of Computer Science, The University of Manchester. He had a postdoctoral position at the Faculty of Electrical Engineering and Computer Science, VSB Technical University of Ostrava, Ostrava, Czech Republic. He is currently a Lecturer at the University of Salford, U.K. He has more than 50 publications in international journals, conferences, and book chapters. In addition, he has five edited books. He has successfully supervised four M.Sc. students and he is currently supervising Ph.D. and M.Sc. students in information security and wireless sensor networks. His major research interests include pattern recognition, cyber security, mobile authentication, machine learning, wireless sensor networks, and biometric authentication. He is a member of The Scientific Research Group in Egypt (SRGE). He has served as the co-chair and PC member in many international conferences and reviewed many scientific papers and participated in many scientific events (national/international conferences and workshops).

SUNIL VADERA received the Ph.D. degree in computer science from The University of Manchester, in 1992. He is currently a Professor of computer science at the University of Salford, U.K., where he has served in many leadership roles including as the Dean and the Head of the School of Computing, Science and Engineering, from 2011 to 2019. He leads the University of Salford's contribution to the Greater Manchester AI Foundry, a project that aims to support SMEs to develop innovative products using AI. His research interests include cost-sensitive learning and deep learning, where he is studying methods of reducing the size of the neural networks. He is a fellow of the British Computer Society, a Chartered Engineer (C.Eng.), and the Chartered IT Professional (CITP). He was awarded the U.K. BDO Best Indian Scientist and Engineer, in 2014, in recognition of his contributions to computing, science and engineering in the U.K. He was the Chair of the U.K. BCS Knowledge Discovery and Data Mining Symposium, Salford, in 2009, and has been the General Chair for numerous conferences including: the IFIP Conference on Intelligent Information Processing, in 2010, 2012, 2014, and 2016; and the International Conference on Information Management and Engineering (2015–2020). He was the Organizing Chair of a Workshop on Cost Sensitive Learning at the IEEE International Conference on Data Mining, in 2012.

KHALED SHAALAN received the B.Sc. degree in computer science (artificial intelligence and software engineering), the M.Sc. degree in informatics, the M.Sc. degree in IT management, and the Ph.D. degree in computer science. He is currently the Head of Programs. He is also a Full Professor of computer science with The British University in Dubai, United Arab Emirates (UAE). He is also an Honorary Fellow with the School of Informatics, The University of Edinburgh, U.K. He has a long experience in teaching in computer science for both core and advanced undergraduate and postgraduate levels. He has taught more than 30 different courses at the undergraduate and postgraduate levels. Over the last two decades, he has been contributing to a wide range of research topics in Arabic natural language processing, including machine translation, parsing, spelling, and grammatical checking, named entity recognition, and diacritization. Moreover, he has also worked on topics in knowledge management, knowledge-based systems, knowledge engineering methodology, including expert systems building tools, expert systems development, and knowledge verification. Nevertheless, he worked on health informatics topics, including context-aware knowledge modeling for decision support in e-health and game-based learning. Furthermore, he worked in educational topics, including intelligent tutoring, item banking, distance learning, and mobile learning. He has been the Principal Investigator or Co-Investigator on research grants from USA, U.K., and United Arab Emirates funding bodies. He has published more than 277 refereed publications and the impact of his research using Google Scholar's H-index metric is 45. He has several research publications in his name in highly reputed journals, such as *Computational Linguistics*, the *Journal of Natural Language Engineering*, the *Journal of the American Society for Information Science and Technology*, the IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, *Expert Systems with Applications*, *Software-Practice and Experience*, the *Journal of Information Science*, *Computer Assisted Language Learning*, and the *European Journal of Scientific Research*. His research work is cited extensively worldwide (see his Google Scholar citation indices). He has guided several master's and Ph.D. students in Arabic natural language processing, healthcare, intelligent tutoring systems, and knowledge management. He encourages and supports his students in publishing at highly ranked journals and conference proceedings. He has been actively and extensively supporting the local and international academic community. He has participated in seminars and invited talks locally and internationally, invited to international group meetings, invited to review papers from leading conferences and premier journals in his field, and invited for reviewing promotion applications to the ranks of an Associate and a Full Professor for applicants from both British and Arab Universities. He is the Founder and the Co-Chair of the International Conference on Arabic Computational Linguistic. He is an Associate Editor of *ACM Transactions of Asian and Low-Resource Language Information Processing* Editorial Board and the Association for Computing Machinery.