An investigation into the performances of the Current state-of-the-art Naive Bayes, Non-Bayesian and Deep Learning Based Classifier for Phishing Detection: A Survey

1st Tosin Ige
Dept. of Computer Science
The University of Texas at El Paso
Texas, USA
toige@miners.utep.edu

2nd Christopher Kiekintveld
Dept. of Computer Science
The University of Texas at El Paso
Texas, USA
cdkiekintveld@utep.edu

3rd Aritran Piplai
Dept. of Computer Science
The University of Texas at El Paso
Texas, USA
apiplai@utep.edu

4th Amy Wagler
Dept. of Public Health Science
The University of Texas at El Paso
Texas, USA
awagler2@utep.edu

5th Olukunle Kolade
Office of Naval Research
United State Navy
Pentagon, USA
ookol@unc.edu

***Abstract*—Phishing is one of the most effective ways in which cybercriminals get sensitive details such as credentials for online banking, digital wallets, state secrets, and many more from potential victims. They do this by spamming users with malicious URLs with the sole purpose of tricking them into divulging sensitive information which is later used for various cybercrimes. In this research, we did a comprehensive review of current state-of-the-art machine learning and deep learning phishing detection techniques to expose their vulnerabilities and future research direction. For better analysis and observation, we split machine learning techniques into Bayesian, non-Bayesian, and deep learning. We reviewed the most recent advances in Bayesian and non-Bayesian-based classifiers before exploiting their corresponding weaknesses to indicate future research direction. While exploiting weaknesses in both Bayesian and non-Bayesian classifiers, we also compared each performance with a deep learning classifier. For a proper review of deep learning-based classifiers, we looked at Recurrent Neural Networks (RNN), Convolutional Neural Networks (CNN), and Long Short Term Memory Networks (LSTMs). We did an empirical analysis to evaluate the performance of each classifier along with many of the proposed state-of-the-art anti-phishing techniques to identify future research directions, we also made a series of proposals on how the performance of the under-performing algorithm can improved in addition to a two-stage prediction model**

***Index Terms*—Phishing, malware attack, DDoS Attack, SVM, Naive Bayes, Munitinomial Naive Bayes**

I. Introduction

Phishing is a type of cybercrime in which an individual is lured to divulging sensitive information details through text message, email, or phone conversation by someone posing either as a legitimate institution or a member of a legitimate institution, some of these commonly requested sensitive details which are social security number, password, credit, and banking card details etc are later used to access more sensitive information for a different type of cybercrime which often results in financial loss or identity theft as about 76% of the phishing attacks were credential-harvesting in 2022 according to Digital Information world. A California teenager was able to get sensitive information to access credit card details and withdraw money from his victim's account through his fake "America Online" website which resulted in the first lawsuit filed in 2004. Efficient phishing detection has been challenging as attackers continue to advance their tactics as technologies evolve [96]–[100]. To defraud personnel, all an attacker needs to do is simply clone a legitimate website to create a new website (SCAM Website) which is then used to defraud computerusers.

Email phishing is responsible for 90% of ransomware attacks and for which the average ransom payment in those instances is can be as high as $200,000 (£161,000), and in addition to the fact that organizations that fall victim of ransomware attacks lose a couple of weeks as downtime [55]. The UK Government's Cyber Security Breaches Survey of 2022 had revealed that cyberattacks rose by 38% in 2022 alone compared to 2021 as 83% of businesses and organizations have suffered at least one data breach with Over 3.4 billion phishing emails sent daily. According to the U.S Federal Bureau of Investigation, 2 billion dollars were stolen due to phishing in 2018 alone, 5 billion dollars was stolen in 2019, and 4.7 billion in 2021 [**?**], [5], [66].In 2019, insights Business E-mail Compromise (BEC) announced that about 4.8 million dollars were lost as a result of phishing attacks in 2022, while a cybersecurity research group reported that a whopping 1.6 million dollars were lost in 2019 4.7 billion dollars in 2021

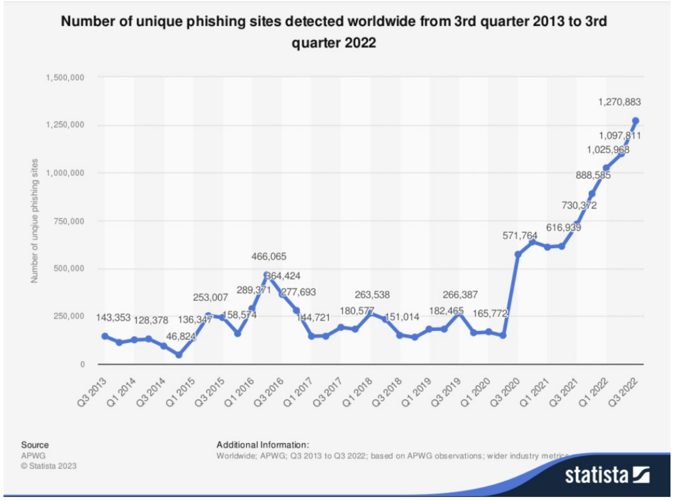

Fig. 1. Phishing statistics from 2013 Q3 to 2022 Q3.

during covid-19 pandemic due to phishing attack.

The ever-evolving ways attacker tries to improve their phishing techniques to bypass existing state-of-the-art anti-phishing detection and prevention method poses a mountain of challenge to researchers in both industry and academia. Thus, the constant evolvement and innovation in phishing techniques adopted by attackers are the reason why all existing anti-phishing methods remain vulnerable to phishing attacks. All existing methods of detecting phishing attack which are based on machine learning [2], [10], [14], [37]–[41], black-lists/whitelists [25], natural language processing [44], visual similarity [44], rules [43], remains vulnerable to attack due to the following reasons;

- Very small or minute changes to the uniform Resource Locator (URL) of a blacklisted URL will make the black-list/ whitelist phishing detection method to fail. Also, the fact that there is no worldwide centralize database for whitelisted or blacklisted URL make this method even more vulnerable, and so if company X blacklisted my phishing URL on their internal server, I can try it with company Y and be successful.
- In machine learning phishing detection which uses relevant features such as URL, webpage content, website traffic, search engine, WHOIS record, and Page Rank has their own vulnerabilities because firstly, such classifier will make a phishing URL that is hosted on a hacked or compromise server to be false classify as benign leading to false negative, secondly using domain age as a feature to train a model will always lead to higher false positive simply because the URL of a newly registered legitimate company website will be misclassify because the domain name was recently register, page rank is zero, and with low traffic, and thirdly the fact that parameters for those features are gotten from third party website is another concern. What will happen if the third party website is having a downtime?
- The issue with visual similarity-based heuristic method which compares both the pre-stored signature such as images, font styles, page layout, and screenshot and so on of the new website with the old website will have general difficulty in detecting anomaly in a newly hosted phishing site.
- The fact that the majority of the existing machine learning models are trained based on textual features such as "#",".", Internet Protocol address, URL Length, domain levels, and so on from the Uniform Resource Locator (URL) does not help simply because any phisher or attacker with little web technologies can develop what we called "friendly URL" depending on the programming language adopted whether JAVA, C#, Python, PHP or framework to avoid all those features. With a friendly URL, such models are bound to misclassify leading to an increment in false negative rate.

For any Machine learning-based phishing detection method to be effective in real-time combat against phishing attacks, it must address each of the stated reasons above for which existing state-of-the-art anti-phishing techniques continue to be vulnerable as phishing methods continue to evolve in a more sophisticated and innovative way. It is worth noting that past reviews on phishing have been largely based on approaches, classification, and so on. RASHA ZIENI et al. [89] focus their review on list-based, similarity-based, and machine learning-based categories of approaches for phishing detection to identify pending research gap, Angad et al. [58] focus theirs on the advantages and limitations of existing approaches to phishing detection, while also using discussion of related application scenarios as guidance to propose a new method of anti-phishing detection, Yifei Wang [83] categorizes widely used phishing detection methods into seven categories and summarizes them.

In this work, we did an extensive review of some of the most recent works on phishing detection, and state-of-the-art algorithms from the past 5 years in order to investigate the performance of the Naive Bayes algorithm relative to other state-of-the-art algorithms for phishing detection task[90]–[95], and the factors behind those performances to uncover future research direction. Our first strategy was to Isolate Naive Bayes from other algorithms, hence, we categorized state-of- the-art phishing detection classifiers into Naive Bayes-based, Machine learning-based, and Deep learning-based for better analysis. The contributions of our research are stated below;

1) Comparative study of the performance of Naive Bayes relative to other machine learning and deep learning-based state-of-the-art algorithms for phishing detection tasks through a survey of the recently published research works.
2) Investigating and analyzing possible factors behind our findings on the performance of Naive Bayes relative to other machine learning and deep learning-based state-of-the-art algorithms for phishing detection
3) Proposing possible solutions so as to identify future

research direction

The rest of the paper is organized as follows: Section II some of the most common forms of phishing attacks by which several high-profile attacks have been carried out in recent years, Section III is split into 3 subsections of Bayesian-based, Non-Bayesian-based, and Deep Learning-based based on the categories of state-of-the-art phishing detection we are considering, under each subsection, we described existing state-of-the-art algorithm under their category. In section IV, we looked at the current approaches for phishing detection, this section is further divided into two subsections based on the two major categories of phishing detection approaches, so, under each section, we described different phishing detection techniques under each subsection, we also looked at the limitations of the current state of art phishing detection methods, while our findings were analyzed and discussed in section V. Finally, conclusion and possible future research directions based on our findings were presented in section VI.

II. BACKGROUND STUDY

Since it is easier for attackers to exploit human weakness to easily bypass the most advanced state-of-the-art defense system by extracting sensitive credentials and information through phishing. Attackers therefore focused their effort on getting sensitive credentials through phishing emails which are mistaken for legitimate emails by unsuspecting victims. Hence, it is imperative to understand how different phishing technique works in order to proffer a strategic defense solution to effectively detect, prevent or mitigate phishing impact in case of a successful attack. In this section, we analyse the process of the major phishing attack.

A. Email Phishing

Email phishing is a phishing type in which unsuspecting victim is tricked into divulging credential or sensitive information through email [10], [52]. Here the attacker sends phishing code either through email containing a phishing link or malware attachment in such a way that as soon as the victim clicks on the link [21], it will either redirect it to a phishing site or get the system infected by malware. Sensitive credentials getting by this mean can then be use by the attacker to commit series of cybercrimes against the victim or target organization including but not limited to remote malware installation, instigate Denial of service attack, Cyberstalking, identity theft, and can even be sold in the dark market.

B. Spear Phishing

Statistic from Barracuda data shows that a typical organization receives 5 customized spear phishing email each day targeting an individual, and despite the fact that only 0.1% of all emails are spear phishing attacks, 66% of all organization breaches are caused by spear phishing. In this type of attack, the attacker keep tracks of the prospective victim activities [30], [72] in the social media such as X formally Twitter, Linkedin, Facebook, Instagram and so on so as to gather substantial information about the targeted victim. With this newly gathered information, the attacker is able to compose email messages which will seems to come from the organization's manager account and typically requesting for sensitive information belonging to the organization.

C. Voice Phishing (Vishing)

It is a type of cybercrime in which attacker make automated phone call by a seemingly legitimate phone number from an organization to get confidential detail from unsuspecting victim [22]. An instance is a customer who get a warning call from an attacker who posed to be bank staff claiming u usual activities on the victim's account and requesting for recently generated one-time password (OTP) or Personal Identification Number (PIN) of the account. The fact that the phisher was able to make scam call from an organization which the victim has connection with makes gives this type of attack a high success rate as experienced in 2021 when 59.49 million which is a whopping 23% of the America population lost an estimated 29.8 billion US Dollar to voice phishing according to earthweb.

D. SMS Phishing (Smishing)

It is a type of cybercrime in which a bait message is sent by an attacker to a set of targeted audience through text message. Messages in a smishing attack usually contains either an email to contact, phone number to call, or link to click where the potential victim is then to provide person credential information such as credit card details, password etc for later use by the attacker on legitimate website to commit series of cybercrime. The SMS uses series of social engineering tactics to ensure potential victim follow the instruction by calling the phone number, contacting the email, or clicking on the link which will lead to the actual phishing website with a form to collect their personal data.

III. CATEGORY OF CURRENT STATE OF THE ART PHISHING DETECTION MODEL

A. Bayesian-Based-Classifier

Naive Bayes is a family of probabilistic-based algorithms that is based on the Bayes rule. It is based on the fact that, if B has occurred, we can find the probability that A will occur. B is taken to be the evidence while the hypothesis is A and with a strong assumption that each of the features is independent. It uses the prior probability distribution to predict the posterior probability of a sample that belongs to a class. In this process, the class with the highest probability is then selected as the final predicted class [84]. Naive Bayes updates prior belief of an event occurring given that there is new information. Hence, given the availability of new data, the probability of the selected sample occurring is given by;

$$P\,(class/features) \;=\; \frac{P\,(class) \,*\, P\,(features/class)}{P\,(features)}$$

Where

- P(class/features) : Posterior Probability

- P(class) : Class Prior Probability
- P(features/class) : Likelihood
- P(features) : Predictor Prior Probability

It has a very strong assumption of independency which affects its performance for classification tasks [36] as the strong assumption of independence among features is not always valid in most of the dataset that is used to train the current state-of-the-art model for several classification tasks. The strong assumption of the Naive Bayes classifier is one reason why it usually underperforms when compared with its peers for similar classification tasks. Naive Bayes classifier has different variants with each variant having its own individual assumption which also impacts its performance in addition to the general assumption of independence which is common to all variants of the Naive Bayes classifier, and so each variant is suitable for different classification tasks.

Multinomial Naive Bayes is a variant of Naive Bayes, It assumes multinomial distribution among features of dataset in addition to the general assumption of independency, and so its performance is affected if the actual distribution is not multinomial or partially multinomial. Multinomial Naive Bayes is the suitable variant for natural language processing classification task [35] but still underperforms when compared with non-bayesian and deep learning-based classifiers for the same NLP classification task.

Gaussian Naive Bayes is the suitable Bayesian variant for anomaly detection in network intrusion which could be used to detect Distributed Denial of Service (DDOS) attacks [36]. It assumes the normal distribution among features in dataset in addition to the general assumption of independence which is common to all variants of Naive Bayes.

Despite being a suitable Naive Bayes variant for anomaly detection, it still underperforms when compared with its suitable peer for detection of Distributed Denial of Service (DDOS) attack as evident in the work done by Rajendran [65] where Gaussian Naive Bayes have the least accuracy of 78.75% compared with other non-bayesian based for attack detection classification task.

Bernoulli Naive Bayes assumes Bernoulli distribution in addition to the assumption of independence. Its main feature is that it only accepts binary values such as success or failure, true or false, and yes or no as input while complement Naive Bayes is used for imbalance datasets as no single variant of Naive Bayes can do the task of all the variants. Both the suitability and performance of each variant are determined by their individual assumption in addition to the general assumption of independence which impacts their performance when compared with their suitable peer for the same classification task.

B. Non-Bayesian Based Classifier

1) Decision Tree: A decision Tree is a Supervised learning technique whose operation is based on a tree-structured classifier, with features in the dataset being represented by an internal node, each decision rule is represented by the branches, while the internal nodes represent the features of a dataset, branches represent the decision rules and each leaf node represents the decision outcome is represented by the leaf node and so does not have further branches. It makes a decision-based graphical representation of all possible solutions to a problem. It uses the Classification and Regression Tree algorithm (CART) [88] to construct a decision tree starting with the root node whose branch keeps expanding further to construct a tree-like structure. It is a non-parametric and the ultimate goal is the creation of a machine learning model capable of making prediction by learning simple decision rules that are inferred from data features.

2) Random Forest: It is an ensemble-based learning algorithm that could be used for classification, regression task, and other similar tasks that operates based on the construction of multiple decision trees [33]. Since the algorithm works by constructing multiple decision trees during training, the output of a classification model trained with a random forest algorithm is the class selected by most of the trees, while the mean or average prediction of individual trees is returned as the output for a regression task. This system of aggregating and ensemblement with multiple trees for prediction makes it possible for a random forest-trained model to outperform the decision tree-trained model and also avoid overfitting which is a peculiar problem for decision tree classifiers.

3) Logistic Regression: Logistic regression is the modeling of the probability of a discrete outcome by having the event log-odds be a linear combination of one or more independent variables given an input variable [23]. Logit transformation is applied to the bounded odds which is the division between the probability of success and probability of failure based on it's linear regression that could be used for both classification and regression tasks and since the output is a probability, the dependent variable is bounded between 0 and 1 values, it uses logistic function to model binary output for classification problems. The difference between linear regression and logistic regression is that the range in logistic regression is bounded by 0 and 1, and also that logistic regression does not require a linear relationship between input and output.

4) XGBoost: It is a supervised learning algorithm that is gradient boosting based. It is extremely efficient and highly scalable, the algorithm works by first creating a series of individual machine learning models and then combining each of the previously created models to form an overall model that is more accurate and efficient than any of the previously created individual models in the series. This system of creating a series of models and combining them to create a single model [26] makes XGBoost perform better than other state-of-the-art machine learning algorithms in many classification, ranking, several user-defined prediction problems, and regression tasks across several domains. XGboost uses gradient descent to add additional individual models to the main model for prediction, hence it is also known as stochastic gradient boosting, gradient boosting machines, or multiple additive regression trees.

5) K-Nearest Neighbor (KNN): k-nearest neighbors (kNN) algorithm is a non-parametric supervised learning algorithm that uses the principle of similarity to predict the label or value of a new data point by considering values of its K-nearest neighbors in the training dataset based on a distance metric like Euclidean distance.

$$\mathrm{dist}(x, z) \leq \mathrm{dist}(x, y) + \mathrm{dist}(y, z) \tag{1}$$

for which the distance between x and z could be calculated by

$$d(x, z) = \sqrt{\sum_{i=1} (x_i - z_i)^2} \tag{2}$$

The prediction of the new data point is based on the average or majority vote of its neighbor, this method allows the classifier to adapt its prediction according to the local structure of the data which ultimately helps to improve its overall accuracy and flexibility. Since KNN can be used for both classification and regression tasks, its prediction output depends on the type of task (classification or regression). In the case of a classification task, it uses class membership as the output by using the plurality vote of its neighbor to assign the input to the class that is most common among its k nearest neighbors, but when KNN is being used for a regression task, it uses the average of the values of k nearest neighbors as the prediction output, the value of k has an impact on the overall accuracy [16] of the model.

6) Support Vector Machine (SVM): Support Vector Machine (SVM) is a supervised machine algorithm that works by looking for a hyper-plane that creates a boundary between two classes of data to solve classification and regression-related problems [28]. It uses the hyper-plane to determine the best decision boundary between different categories in the training dataset, hence they can be applied to vectors that could encode data. Two theories must hold before we can determine the suitability of SVM for certain classification or regression tasks, the first is the availability of high-dimension input space as SVM tries to prevent overfitting by using an overfitting protective measure which is independent of the number of features in the data gives SVM the potential to handle feature spaces in the dataset. The second theory is the presence of linearly separable properties of categorization in the training dataset, and this is because SVM works by finding linear separators between each of the categories to make accurate predictions.

C. Deep Learning Based Classifier

1) Convolutional Neural Network (CNN): CNN is a deep learning model with a grid pattern for processing data that is designed to automatically and adaptively learn spatial hierarchies of features, from low- to high-level patterns [?]. It is a mathematical construct that is composed of convolution, pooling, and fully connected layers as three types of layers or building blocks responsible for different tasks for predictions. While convolution and pooling layers, perform feature extraction, the fully connected layer, maps the extracted features into the final output usually known as classification. The convolution layer is composed of mathematical operations (convolution) which plays a very crucial role in Convolutional Neural Networks as in a kind of linear operation. The CNN architecture is a combination of several building blocks like convolution layers, pooling layers, and fully connected layers, and so, a typical architecture consists of repetitions of a stack of many convolution layers and a pooling layer, and then followed by one or more fully connected layers. It stored digital images, and pixel values as a two-dimensional (2D) grid which is an array of numbers along with some parameters called the kernel before an optimizable feature extractor is finally applied at each image position. This makes CNNs a highly efficient classifier for image processing classification tasks, since a feature may occur anywhere in the image. extracted features can hierarchically and progressively become more complex as each layer progressively feeds its output to the next layer, the main task is the minimization of differences between output and ground truth by backward propagation and gradient descent which is an optimization algorithm. This process of optimizing parameters like kernels to minimize the difference between outputs and ground truth is called training.

2) Recurrent Neural Network (RNN): Recurrent Neural Networks (RNNs) is a type of Neural Network in which output from the previous step is fed to the current step as input, It introduce the concept of memory to neural networks through the addition of the dependency between data points. This addition of dependency between data points ensured that RNNs could be trained to remember concepts by able able to learn repeated patterns. The main difference between RNN and the traditional neural network is the concept of memory in RNN which is made possible as a result of the feedback loop in the cell. Here, it is the feedback loop that enables the possibility of passing information within a layer unlike in feedforward neural networks where information can only be passed between layers. While input and output are independent of each other in a traditional neural network, It is a different ball game in RNN where sequence information is to be remembered, this was made possible in RNN by its Hidden state also known as the memory state through which it remembers previous input to the network, and so it is safe to conclude that the most important features of RNNs is the Hidden state by which it remembers some information in a sequence. In terms of architecture, RNN architecture is the same as that of other deep neural networks, the main difference lies in how the information flows from the input to the output. While the weight across the network in RNN is the same, deep neural network has different weight matrices for each dense network. The Hidden state in the RNNs which enables them to remember sequence information makes it suitable for natural language processing tasks.

3) Long Short-Term Memory (LSTM): Long short-term memory (LSTM) network is a recurrent neural network (RNN) that is specifically designed to handle sequential data, such as speech, text, and time series, it is aimed at solving the problem of vanishing gradient in traditional RNNs. It is insensitive to gap length which gives it an advantage over hidden Markov models, hidden Markov models, and other RNNs. It provides

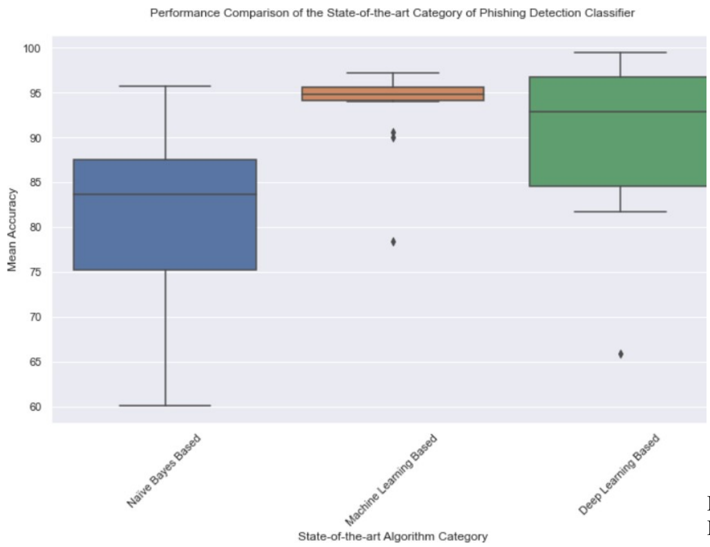

Fig. 2. Comparative Analysis of State-of-the-art Phishing Algorithm for Phishing Detection.

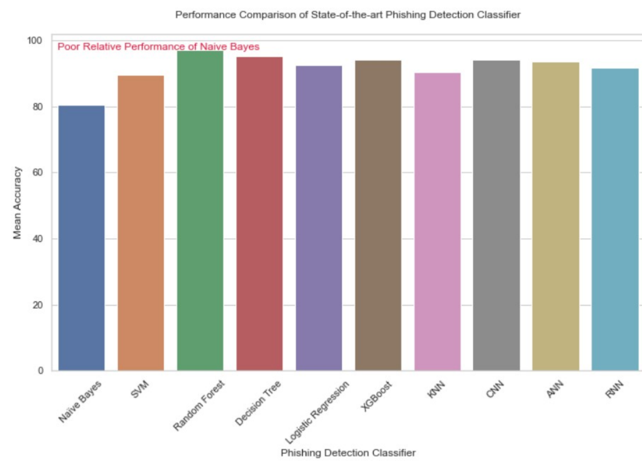

Fig. 3. Comparative Analysis of State-of-the-art Phishing Algorithm for Phishing Detection.

a short-term memory for RNN which can last thousands of timesteps thereby making it a ”long short-term memory” network. A single LSTM network unit is composed of an output gate, a cell, an input gate, and a forget gate. While the three gates regulate the flow of information into and out of the cell, the cell is responsible for remembering values over arbitrary time intervals as the Forget gates decide on the information to discard from a previous state by assigning a previous state, compared to a current input which assigns a value between 0 and 1. A value of 1 means the information is to be kept, and a value of 0 means the information is to be discarded. The Input gates decide on the exact pieces of new information to store in the current state in the same way as forget gates. Output gates consider both the previous and current states to control which pieces of information in the current state are to output by assigning a value from 0 to 1 to the information. This selective outputting of relevant information from the current state allows the LSTM network to utilize both useful and long-term dependencies in making more accurate predictions in current and future time steps. The fact that they are designed to learn long-term dependencies in sequential data makes them suitable for time series forecasting, speech recognition, and language translation tasks.

IV. Discussion and Analysis

Our initial decision was to use a combination of f1 score, precision, and accuracy as a performance evaluation metric, but when searching for an appropriate evaluation metric that we could use, we observed that the overwhelming majority of the authors rely solely on accuracy as a measure of evaluation, this shaped our decision to use evaluation as a criterion for performance measurement, and as we all know that there is no single perfect evaluation metric meaning that accuracy alone is not a perfect evaluation metric because different factors and condition can affect the accuracy like imbalance in the dataset which could tilt the accuracy in favor or against a classifier, preprocessing (where roles containing null values were removed or replaces), bias in dataset, possible mistake or negligence on the part of the author and so on. To ensure fairness and a true picture of the performance of individual state-of-the-art algorithms for phishing detection tasks, we decided to use mean accuracy both at individual and categorical levels.

Having adopted mean accuracy as a measure of performance evaluation to counter the effect of (i) uncertainty in the quality of dataset since they come from a different source in which some are internally generated in certain cases and not available as a public dataset (ii) dataset imbalance or bias that can tilt the result in favor or against a target (iii) series of processing tasks such as complete removal of rows with null values that can cause massive reduction in dataset or replacing them with the mean value which makes the data distorted and not exact (iv) unintended mistake or negligence as every researcher is different in terms of professionalism, ethical level, attention to details. We tried to look at the reason why phishing is still very effective despite the accuracy and performances of machine learning models, hence, we observed the following;

(1) Overwhelming reliance on the Uniform Resource Locator(URL) dataset

It is worth noting that current state-of-the-art machine-learning phishing detection models are trained based on the properties of the URL such as length of URL, length of the hostname, average words in URL, longest words, character repetition, average path, who is registered domain, domain with copyright, domain age, web traffic, DNS record, google index, PageRank and so on. To better understand why successful phishing attack remains high despite the level of accuracy from state-of-the-art machine learning-based phishing detection model, we will classify the properties of

TABLE I

LIMITATIONS OF CURRENT STATE-OF-THE-ART METHODS FOR PHISHING DETECTION

Author	Dataset	Research Summary	Method/Algorithm	Limitation
Ann Zeky et al (2023) [53]	internally generated dataset	proposal of extraction based naive Bayes robust model for phishing detection with emphasis on a combination of webpage content and URL feature analysis	naive Bayes URL analyzation webpage content extraction	1. problem of bayesian poisoning was not addressed and so the model remains vulnerable to bayesian poisoning
mahdi bahaghighat (2023) [17]	Public URL Dataset	performance comparison of phishing detection method based on several six different algorithm	naive bayes KNN SVM Random Forest Gradient Boost Logistic Regression	1. complexity of re-generating tree for every output in random forest remains 2. sole reliance on URL feature attributes means the model remains vulnerable to friendly URL
Nishitha U et al (2023) [60]	Review	performance comparison of machine learning and deep learning based algorithm for phishing detection	CNN RNN KNN Random Forest Decision Tree Logistic Regression	1. 5000 records is too small to train a CNN model and so no confidence here 2. imbalance in the dataset will lead to bias sole reliance on URL feature
Santhosh Raminedi et al (2023) [67]	public URL dataset	evaluation of several machine learning and deep learning based algorithms for phishing detection using URL features	ANN SVM KNN and Naive Bayes Random Forest Decision Tree Logistic Regression	1. complexity of generating tree for every output in random forest was not addressed 2. sole reliance on URL feature
Palla Yaswanth and V. Nagaraju (2023) [85]	phishing dataset	novel network prediction of phishing sites based on optimal hyper-parameter turning and comparison of the performances of Bayesian and Random Forest Classifier for Phishing Detection	Naive Bayes and Random Forest	1. No investigation or hint on the cause of the 5% failure rate 2. heavy reliance on parameter turning 3. Limited dataset
Abdul Karim et al (2023) [47]	public URL dataset	proposal of hybrid model with a combination of logistic regression, support vector machine, and decision tree along with a combination of soft and hard voting for efficient defense against phishing attack	Decision Tree Logistic Regression Support Vector Machine Soft and Hard voting	1. sole reliance on the URL attribute means the proposed model will be vulnerable to a phishing website with legitimate friendly URL 2. user have to manually surf the internet to get essential URL parameter from a third party to feed the model which is cumbersome and might not be available
Ishwarya et al (2023) [42]	Kaggle email dataset	Proposal of a phishing detection method and performance comparison of Naive Bayes, SVM, KNN, and random forest classifier for phishing detection	naive bayes KNN SVM Random Forest	1. use of an imbalance dataset of 87% ham and 13% spam which was not addressed 2. Vulnerability to Bayesian poisoning
Kamal Omari (2023) [61]	UCL Phishing Dataset	an investigation into the performances and efficiency of Logistic Regression, KNN, SVM, Naive Bayes, Decision Tree, Random Forest, and Gradient Boosting for phishing detection task	naive bayes KNN SVM Random Forest Gradient Boost Decision Tree Logistic Regression	1. While Random Forest have a good accuracy of 97.1%, its complexity of regenerating tree still remains 2. Heavy reliance on URL attributes which means the model remains vulnerable
Twana Mustafa and Murat Karabatak (2023) [59]	UCL phishing dataset	Performance Comparison of different Bayesian classifier based on different Feature Selection Algorithm	naive bayes individual FS forward FS backward FS Plus-I takeaway-r FS AR1 FS	1. each of the Bayesian model remains vulnerable to Bayesian poisoning no hint on why Plus-I takeaway-r FS works better best for naive bayes
Jaya T et al (2023) [45]	UCL phishing dataset	usage of frequency weightage of the words for unsupervised clustering of mail into spam and ham messages	naive bayes random forest logistic regression random tree LTSM	1. while random forest performed really well, its complexity of generating tree for every output remains a problem possible reason for the poor performance of Bayesian classifier remains to be investigated

the phishing URL on which ML models are being trained into Controllable Properties and Uncontrollable Properties.

(a) Controllable Property:
We classified controllable properties of URLs as properties or characteristics of URLs that could be controlled by attackers.URL characteristics such as length of URL, length of the hostname, average URL, longest word, character repetition, average word, average path, etc can easily be defeated by using SEARCH ENGINE FRIENDLY URL.

TABLE II
COMPARISON OF DIFFERENT CATEGORIES OF THE STATE-OF-THE-ART PHISHING DETECTION METHODOLOGIES

Category of Methodologies	Authors	Average Accuracy
Naive Bayes-Based	[17], [67], [85], [47], [61], [6], [7], [1], [62], [80], [69], [74], [71], [13], [50]	78.62, 61.0, 95.58, 88.39, 60.1, 95.67, 79.7, 85.15, 83.46, 74.02, 83.88, 92.94, 84.10, 73.8, 70.05
Machine Learning-Based	[17], [67], [85], [47], [61], [12], [6], [8], [68], [15], [63], [79], [70], [46]	95.4, 94.9, 94.6, 78.4, 95.5, 95.7, 96.4, 90.63, 94.7, 94.5, 94.0, 90.0, 97.2, 96.27
Deep Learning-Based	[67], [12], [8], [79], [34], [9], [3], [4], [34], [24], [77], [19], [64], [73]	88, 95, 97.4, 93.0, 81.75, 95.02, 92.67, 92.19, 65.9, 99.2, 99.5, 82.0, 83.38, 97.63

Except the attacker is not experienced, an experienced attacker will know how the ML model works, and so having a slight experience in web technology will enable a phisher to bypass models that are trained based on the controllable properties of the phishing URL, so the outcome of those models inreal-time application after deployment will be an extremely high rate of false negative, and we know that having a high rate of false negative means users will be lead to the phishing site where their credentials will be taken by the attacker.

(b) Uncontrollable Property:
We describe them as properties of URLs that cannot be controlled, they build and accumulate over the years. Properties such as domain age, web traffic, Google Index, and PageRank take years to build and accumulate. Hence, for a newly incorporated legitimate business, the website will be relatively fresh and so, properties of their site URL will be very low on these properties, meaning that they will be classified as a phishing website thereby leading to a very high rate of false positive, such ML model are bound to put newly registered legitimate business with quality product and services to offer, startups at a very big disadvantage as their URL will be incorrectly classified or flagged as phishing site.

There is a need for significant improvement in training for the existing state of art ML-based model to be truly effective in real-time phishing detection, for this purpose, we proposed combined use of the controllable properties of the URL with web scrapping. Using Uncontrollable properties like the length of the URL, length of the hostname, average URL, longest word, character repetition, average word, average path, etc which takes many years to form will tilt the prediction of the model against recently incorporated legitimate businesses and startups as their site URL will be incorrectly classified as phishing in real-time usage, hence, we suggested the use of the controllable characteristics of site URL along with background web scraping is the background extraction of data from the URL. As attackers have recently resorted to using images on their phishing sites to avoid detection, we are proposing a two-stage prediction model where random forest makes the first prediction based on the properties of the URL, and if the first stage is successful i.e the site is predicted as legitimate, then the model goes to the next stage of prediction where the content of the URL is web scrapped and fed to a Convolutional Neural Network to make the final prediction.

We chose Random Forest for the first stage because it outperformed other machine learning models with a mean accuracy of 97% for phishing detection using properties or characteristics of the URL, while we chose CNN due to its effectiveness in natural language processing tasks and image classification. We believe that a two-staged ensemble model consisting of a Random Forest and a Convolutional Neural Network for phishing detection will significantly improve current state-of-the-art phishing detection without jeopardizing the interest of new startups whose domains are relatively new. .

(2) Overral Poor performance of Naive Bayes at each level
Before any solution can be proposed, it is worth going down memory lane to look at the various assumption of Naive Bayes classifier and its variants, and having affirmed that each Na¨ıve Bayes variants performances and accuracy is largely due to its assumption, Gaussian variant is suitable for anomaly detection due to its assumption that features follow continuous normal distributions, Bernoulli Nave Bayes assumes binomial distribution while multinonial Naive Bayes variant have a dismal performance due to its assumption of discreet multinomial distribution [36], [35], this was also evident during Investigation of the impact of correlation between dataset features on machine learning models for malware classification task [76] where Gaussian Naive Bayes have outlinear performance relative to other classifiers, so each variant of Naive Bayes classifier is parametric based on its individual assumption of feature ditribution in dataset in addition to the generic assumption of independency among feature which rarely holds in real dataset.

The current way of improving the performance of naive Bayesian classifiers is the relaxation of the fundamental assumption of independence among individual attributes in the dataset, which is usually done by an estimation of the joint probability density function (PDF) instead of using the conventional marginal probability density function which is non-naive [82]. The problem with this approach is that it only gives a slight improvement over the conventional naive Bayes due to the adoption of a joint probability density function, the actual association among the features is not preserved.

We propose regularization to the current Bayes Rule that will put (i) the level of correlation or dependency among the features and (ii) the underlying nature of feature distribution in the dataset into perspective as a way to improve the performance of Naive Bayes-based algorithms. This will invariably lead to a new variant of the Naive Bayes classifier with superior performance compared with the existing variants

TABLE III
COMPARISON OF DIFFERENT ALGORITHMS FOR PHISHING DETECTION TASK

Classifier	Category	Authors	Accuracy	Average Accuracy
Multinomial NB	Naive Bayes	[17], [67], [85], [47], [61], [6], [7], [1], [62], [80], [69], [74], [71], [13], [50]	78.62, 61.0, 95.58, 88.39, 60.1, 95.67, 79.7, 85.15, 83.46, 74.02, 83.88, 92.94, 84.10, 73.8, 70.05	80.431
SVM	Machine Learning	[17], [67], [47], [61], [12], [6], [68], [15], [63], [81], [48], [13]	94.43, 94, 71.8, 93.9, 94.0, 94.45, 94.0, 96.4, 95.97, 90.6, 94.0, 59.6	89.429
Random Forest	Machine Learning	[17], [67], [85], [47], [61], [11], [12], [6], [63], [8], [68], [70], [48]	97.10, 97, 94.6, 96.77, 97.1, 98.11, 97.0, 97.98, 99.13, 94.26, 97.0, 98.6, 97.2	97.065
Decision Tree	Machine Learning	[67], [47], [61], [12], [6], [68], [63], [57], [48], [62], [80], [13]	96.41, 94.9, 96.3, 96.0, 97.02, 93.0, 92.26, 97.62, 95.9, 96.3, 93.57, 93.7	95.248
Logistic Regression	Machine Learning	[17], [67], [61], [15], [63], [79], [70], [48], [51], [1], [62]	93.16, 92.28, 92.7, 93.4, 92.67, 86.0, 95.9, 96.9, 94.7, 94.18, 86.59	92.589
XGBoost	Machine Learning	[17], [47], [61], [6], [62], [80], [17], [27], [71], [54], [13]	96.93, 70.34, 97.2, 96.64, 97.88, 94.79, 99.2, 98.75, 90.83, 96.71, 96.40	94.152
KNN	Machine Learning	[17], [67], [47], [61], [6], [8], [15], [63], [79], [70], [20], [48], [80], [13]	95.36, 94.75, 58.63, 95.6, 95.67, 87.0, 93.6, 95.20, 94.0, 97.16, 96.0, 97.2, 83.33, 83.20	90.479
CNN	Deep Learning	[34], [32], [9], [87], [3], [86], [4], [77], [19]	97.6, 96.8, 95.02, 92.01, 92.55, 98.2, 92.35, 99.43, 84	94.218
ANN	Deep Learning	[67], [12], [79], [56], [64], [73], [31], [75], [49], [50]	88.0, 95.0, 93.0, 98.72, 83.38, 97.63, 97.6, 97.26, 97, 88.22	93.581
RNN	Deep Learning	[8], [34], [3], [4], [29], [24], [18], [77], [19], [78]	97.4, 65.9, 92.79, 92.03, 96.74, 99.2, 98.7, 99.57, 80, 93.9	91.623

of the Bayesian classifier.

V. CONCLUSION AND FUTURE RESEARCH DIRECTION

In this work, we did an extensive review of some of the most recent works on phishing detection, and state-of-the-art algorithms from the past 5 years in order to investigate the performance of Naive Bayes algorithm relative to other state-of-the-art algorithms for phishing detection task, and the factors behind those performances to uncover future research direction. In our comparative study of the performance of Naive Bayes relative to other machine learning and deep learning-based state-of-the-art algorithms for phishing detection tasks through a survey of the recently published research papers, Random Forest, Decision Tree, CNN, XGBoost with an individual mean accuracy of 97.1%, 95.2%, 94.2%, and 94.1% respectively have the top 4 performance for URL properties-based phishing detection task while Naive Bayes, SVM, RNN with individual mean accuracy of 80.4%, 89.4%, and 91.6% respectively have the worst 3 performance for URL properties-based phishing detection classification task.

In our effort to improve the performance of current state-of-the-art phishing detection methods that rely on the properties of the phishing URLs, especially to counter the ever-evolving phishing methods in which attackers are now using images as text to avoid detection, we proposed a two-stage prediction model where random forest makes the first prediction base on the properties of the URL, and if the first stage is successful i.e the site is predicted as legitimate, then the model goes to the next stage of prediction where the content of the URL is web scrapped and fed to a Convolutional Neural Network to make the final prediction. We chose Random Forest for the first stage because it outperforms other classifiers for phishing detection based on URL properties while CNN was chosen due to its effectiveness in natural language processing and image classification tasks.

Looking at the poor performance of the Naive Bayes classifier both at the individual and categorical levels for which it has the least performance for phishing detection classification task, we propose regularization to the current Bayes Rule that will put both the level of correlation or dependency among the features as well as the underlying nature of feature distribution in a dataset into perspective as a way to improve the performance of Naive Bayes-based algorithms instead of just ignoring them or merely replacing the marginal probability density function with joint probability density function as seen in non-naive Bayes.

REFERENCES

[1] Mohd Faizal Ab Razak, Mohd Izham Jaya, Ferda Ernawan, Ahmad Firdaus, and Fajar Agung Nugroho. Comparative analysis of machine learning classifiers for phishing detection. In *2022 6th International Conference on Informatics and Computational Sciences (ICICoS)*, pages 84–88. IEEE, 2022.

[2] Lozan Mohammed Abdulrahman, Sarkar Hasan Ahmed, Zryan Najat Rashid, Yousif Sufyan Jghef, Teba Mohammed Ghazi, and Umed H Jader. Web phishing detection using web crawling, cloud infrastructure and deep learning framework. *Journal of Applied Science and Technology Trends*, 4(01):54–71, 2023.

[3] Moruf A Adebowale, Khin T Lwin, and M Alamgir Hossain. Deep learning with convolutional neural network and long short-term memory for phishing detection. In *2019 13th International Conference on Software, Knowledge, Information Management and Applications (SKIMA)*, pages 1–8. IEEE, 2019.

[4] Moruf Akin Adebowale, Khin T Lwin, and Mohammed Alamgir Hossain. Intelligent phishing detection scheme using deep learning algorithms. *Journal of Enterprise Information Management*, 36(3):747–766, 2023.

[5] Sikiru Adewale, Tosin Ige, and Bolanle Hafiz Matti. Encoder-decoder based long short-term memory (lstm) model for video captioning. *arXiv preprint arXiv:2401.02052*, 2023.

[6] Md Abdullah Al Ahasan, Mengjun Hu, and Nashid Shahriar. Ofmcdm/irf: A phishing website detection model based on optimized fuzzy multi-criteria decision-making and improved random forest. In *2023 Silicon Valley Cybersecurity Conference (SVCC)*, pages 1–8. IEEE, 2023.

[7] Mustafa Al Fayoumi, Ammar Odeh, Ismail Keshta, Abobakr Aboshgifa, Tareq AlHajahjeh, and Rana Abdulraheem. Email phishing detection based on na¨ıve bayes, random forests, and svm classifications: A comparative study. In *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 0007–0011. IEEE, 2022.

[8] Eman Abdullah Aldakheel, Mohammed Zakariah, Ghada Abdalaziz Gashgari, Fahdah A Almarshad, and Abdullah IA Alzahrani. A deep learning-based innovative technique for phishing detection in modern security with uniform resource locators. *Sensors*, 23(9):4403, 2023.

[9] Ali Aljofey, Qingshan Jiang, Qiang Qu, Mingqing Huang, and Jean-Pierre Niyigena. An effective phishing detection model based on character level convolutional neural network from url. *Electronics*, 9(9):1514, September 2020.

[10] Ali Aljofey, Qingshan Jiang, Abdur Rasool, Hui Chen, Wenyin Liu, Qiang Qu, and Yang Wang. An effective detection approach for phishing websites using url and html features. *Scientific Reports*, 12(1):8842, 2022.

[11] Mohammad Almseidin, AlMaha Abu Zuraiq, Mouhammd Al-Kasassbeh, and Nidal Alnidami. Phishing detection based on machine learning and feature selection methods. 2019.

[12] Shouq Alnemari and Majid Alshammari. Detecting phishing domains using machine learning. *Applied Sciences*, 13(8):4649, 2023.

[13] Safa Alrefaai, Ghina Özdemir, and Afnan Mohamed. Detecting phishing websites using machine learning. In *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, pages 1–6. IEEE, 2022.

[14] J Anitha and M Kalaiarasu. A new hybrid deep learning-based phishing detection system using mcs-dnn classifier. *Neural Computing and Applications*, pages 1–16, 2022.

[15] M Arivukarasi, A Manju, R Kaladevi, Shanmugasundaram Hariharan, M Mahasree, and Andraju Bhanu Prasad. Efficient phishing detection and prevention using support vector machine (svm) algorithm. In *2023 IEEE 12th International Conference on Communication Systems and Network Technologies (CSNT)*, pages 545–548. IEEE, 2023.

[16] Tsehay Admassu Assegie. K-nearest neighbor based url identification model for phishing attack detection. *Indian Journal of Artificial Intelligence and Neural Networking*, 1:18–21, 2021.

[17] Mahdi Bahaghighat, Majid Ghasemi, and Figen Ozen. A high-accuracy phishing website detection method based on machine learning. *Journal of Information Security and Applications*, 77:103553, 2023.

[18] Alejandro Correa Bahnsen, Eduardo Contreras Bohorquez, Sergio Villegas, Javier Vargas, and Fabio A González. Classifying phishing urls using recurrent neural networks. In *2017 APWG symposium on electronic crime research (eCrime)*, pages 1–8. IEEE, 2017.

[19] Eduardo Benavides-Astudillo, Walter Fuertes, Sandra Sanchez-Gordon, German Rodriguez-Galan, Verónica Martínez-Cepeda, and Daniel Nuñez-Agurto. Comparative study of deep learning algorithms in the detection of phishing attacks based on html and text obtained from web pages. In *International Conference on Applied Technologies*, pages 386–398. Springer, 2022.

[20] Subba Reddy Borra, B Gayathri, B Rekha, B Akshitha, and B Hafeeza. K-nearest neighbour classifier for url-based phishing detection mechanism. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 14(03):34–40, 2023.

[21] Ladislav Burita, Petr Matoulek, Kamil Halouzka, and Pavel Kozak. Analysis of phishing emails. *AIMS Electronics and Electrical Engineering*, 5(1):93–116, 2021.

[22] Debra L Cook, Vijay K Gurbani, and Michael Daniluk. Phishwish: a stateless phishing filter using minimal rules. In *Financial Cryptography and Data Security: 12th International Conference, FC 2008, Cozumel, Mexico, January 28-31, 2008. Revised Selected Papers 12*, pages 182–186. Springer, 2008.

[23] Thomas W. Edgar and David O. Manz. Chapter 4 - exploratory study. In Thomas W. Edgar and David O. Manz, editors, *Research Methods for Cyber Security*, pages 95–130. Syngress, 2017.

[24] Tao Feng and Chuan Yue. Visualizing and interpreting rnn models in url-based phishing detection. In *Proceedings of the 25th ACM Symposium on Access Control Models and Technologies*, pages 13–24, 2020.

[25] Z Ghaleb Al-Mekhlafi, B Abdulkarem Mohammed, Mohammed Al-Sarem, Faisal Saeed, Tawfik Al-Hadhrami, Mohammad T Alshammari, Abdulrahman Alreshidi, and T Sarheed Alshammari. Phishing websites detection by using optimized stacking ensemble model. *Computer Systems Science and Engineering*, 41(1):109–125, 2022.

[26] Jiaqi Gu and Hui Xu. An ensemble method for phishing websites detection based on xgboost. In *2022 14th international conference on computer research and development (ICCRD)*, pages 214–219. IEEE, 2022.

[27] Eder S Gualberto, Rafael T De Sousa, P De B Thiago, João Paulo CL Da Costa, and Cláudio G Duque. From feature engineering and topics models to enhanced prediction rates in phishing detection. *Ieee Access*, 8:76368–76385, 2020.

[28] Bao Guo, Chunxia Zhang, Junmin Liu, and Xiaoyi Ma. Improving text classification with weighted word embeddings via a multi-channel textcnn model. *Neurocomputing*, 363:366–374, 2019.

[29] Lukáš Halgaš, Ioannis Agrafiotis, and Jason RC Nurse. Catching the phish: Detecting phishing attacks using recurrent neural networks (rnns). In *Information Security Applications: 20th International Conference, WISA 2019, Jeju Island, South Korea, August 21–24, 2019, Revised Selected Papers 20*, pages 219–233. Springer, 2020.

[30] Shuichiro Haruta, Hiromu Asahina, and Iwao Sasase. Visual similarity-based phishing detection scheme using image and css with target website finder. In *GLOBECOM 2017-2017 IEEE Global Communications Conference*, pages 1–6. IEEE, 2017.

[31] Katherine Haynes, Hossein Shirazi, and Indrakshi Ray. Lightweight url-based phishing detection using natural language processing transformers for mobile devices. *Procedia Computer Science*, 191:127–134, 2021.

[32] M Hiransha, Nidhin A Unnithan, R Vinayakumar, K Soman, and ADR Verma. Deep learning based phishing e-mail detection. In *Proc. 1st AntiPhishing Shared Pilot 4th ACM Int. Workshop Secur. Privacy Anal.(IWSPA)*, pages 1–5. Tempe, AZ, USA, 2018.

[33] Mohith Gowda HR, Adithya MV, et al. Development of anti-phishing browser based on random forest and rule of extraction framework. *Cybersecurity*, 3(1):1–14, 2020.

[34] Yongjie Huang, Qiping Yang, Jinghui Qin, and Wushao Wen. Phishing url detection via cnn and attention-based hierarchical rnn. In *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pages 112–119. IEEE, 2019.

[35] Tosin Ige and Sikiru Adewale. Ai powered anti-cyber bullying system using machine learning algorithm of multinomial na¨ıve bayes and optimized linear support vector machine. *arXiv preprint arXiv:2207.11897*, 2022.

[36] Tosin Ige and Christopher Kiekintveld. Performance comparison and implementation of bayesian variants for network intrusion detection. *arXiv preprint arXiv:2308.11834*, 2023.

[37] Tosin Ige, Christopher Kiekintveld, and Aritran Piplai. Deep learning-based speech and vision synthesis to improve phishing attack detection through a multi-layer adaptive framework. *arXiv preprint arXiv:2402.17249*, 2024.

[38] Tosin Ige, Christophet Kiekintveld, and Aritran Piplai. An investigation into the performances of the state-of-the-art machine learning approaches for various cyber-attack detection: A survey. In *2024 IEEE International Conference on Electro Information Technology (eIT)*, pages 135–144. IEEE, 2024.

[39] Tosin Ige, Abosede Kolade, and Olukunle Kolade. Enhancing border security and countering terrorism through computer vision: A field of artificial intelligence. In *Proceedings of the Computational Methods in Systems and Software*, pages 656–666. Springer, 2022.

[40] Tosin Ige, William Marfo, Justin Tonkinson, Sikiru Adewale, and Bolanle Hafiz Matti. Adversarial sampling for fairness testing in deep neural network. *arXiv preprint arXiv:2303.02874*, 2023.

[41] Tosin Ige and Adewale Sikiru. Implementation of data mining on a secure cloud computing over a web api using supervised machine learning algorithm. In *Computer Science On-line Conference*, pages 203–210. Springer, 2022.

[42] R Ishwarya, S Muthumani, Siva Sharma Karthick PG, and S Suriya. Seperation of phishing emails using probabilistic classifiers. In *2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS)*, volume 1, pages 1676–1679. IEEE, 2023.

[43] Ankit Kumar Jain and Brij B Gupta. A novel approach to protect against phishing attacks at client side using auto-updated white-list. *EURASIP Journal on Information Security*, 2016:1–11, 2016.

[44] Ankit Kumar Jain and Brij B Gupta. A machine learning based approach for phishing detection using hyperlinks information. *Journal of Ambient Intelligence and Humanized Computing*, 10:2015–2028, 2019.

[45] T Jaya, R Kanyaharini, and Bandi Navaneesh. Appropriate detection of ham and spam emails using machine learning algorithm. In *2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*, pages 1–5. IEEE, 2023.

[46] Murat Karabatak and Twana Mustafa. Performance comparison of classifiers on reduced phishing website dataset. In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, pages 1–5. IEEE, 2018.

[47] Abdul Karim, Mobeen Shahroz, Khabib Mustofa, Samir Brahim Belhaouari, and S Ramana Kumar Joga. Phishing detection system through hybrid machine learning based on url. *IEEE Access*, 11:36805–36822, 2023.

[48] Mohammad Farhan Khan, Rohit Kumar Tiwari, Sushil Kumar Saroj, and Tripti Tripathi. A comparative study of machine learning techniques for phishing website detection. In *Role of Data-Intensive Distributed Computing Systems in Designing Data Solutions*, pages 97–109. Springer, 2023.

[49] Sohail Ahmed Khan, Wasiq Khan, and Abir Hussain. Phishing attacks and websites classification using machine learning and multiple datasets (a comparative analysis). In *Intelligent Computing Methodologies: 16th International Conference, ICIC 2020, Bari, Italy, October 2–5, 2020, Proceedings, Part III 16*, pages 301–313. Springer, 2020.

[50] Mehmet Korkmaz, Ozgur Koray Sahingoz, and Banu Diri. Detection of phishing websites by using machine learning-based url analysis. In *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pages 1–7. IEEE, 2020.

[51] K Varun Kumar and M Ramamoorthy. Machine learning-based spam detection using na¨ıve bayes classifier in comparison with logistic regression for improving accuracy. *Journal of Pharmaceutical Negative Results*, pages 548–554, 2022.

[52] Yukun Li, Zhenguo Yang, Xu Chen, Huaping Yuan, and Wenyin Liu. A stacking model using url and html features for phishing webpage detection. *Future Generation Computer Systems*, 94:27–39, 2019.

[53] Ann Zeki Ablahd Magdacy Jerjes, Adnan Yousif Dawod, and Mohammed Fakhrulddin Abdulqader. Detect malicious web pages using naive bayesian algorithm to detect cyber threats. *Wireless Personal Communications*, pages 1–13, 2023.

[54] Mukta Mithra Raj and J Angel Arul Jothi. Website phishing detection using machine learning classification algorithms. In *International Conference on Applied Informatics*, pages 219–233. Springer, 2022.

[55] Dietmar PF Möller. Ransomware attacks and scenarios: Cost factors and loss of reputation. In *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices*, pages 273–303. Springer, 2023.

[56] Krishna Mridha, Jahid Hasan, D Saravanan, and Ankush Ghosh. Phishing url classification analysis using ann algorithm. In *2021 IEEE 4th International Conference on Computing, Power and Communication Technologies (GUCON)*, pages 1–7. IEEE, 2021.

[57] Yohan Muliono, Muhammad Amar Ma'ruf, and Zakiyyah Mutiara Azzahra. Phishing site detection classification model using machine learning approach. *Engineering, MAthematics and Computer Science (EMACS) Journal*, 5(2):63–67, 2023.

[58] Amgad Muneer, Rao Faizan Ali, Abdo Ali Al-Sharai, and Suliman Mohamed Fati. A survey on phishing emails detection techniques. In *2021 International Conference on Innovative Computing (ICIC)*, pages 1–6. IEEE, 2021.

[59] Twana Mustafa and Murat Karabatak. Feature selection for phishing website by using naive bayes classifier. In *2023 11th International Symposium on Digital Forensics and Security (ISDFS)*, pages 1–4. IEEE, 2023.

[60] U Nishitha, Revanth Kandimalla, Reddy M Mourya Vardhan, and U Kumaran. Phishing detection using machine learning techniques. In *2023 3rd Asian Conference on Innovation in Technology (ASIANCON)*, pages 1–6. IEEE, 2023.

[61] Kamal Omari. Comparative study of machine learning algorithms for phishing website detection. *International Journal of Advanced Computer Science and Applications*, 14(9), 2023.

[62] Uğur Ozker and Ozgur Koray Sahingoz. Content based phishing detection with machine learning. In *2020 International Conference on Electrical Engineering (ICEE)*, pages 1–6. IEEE, 2020.

[63] Pankaj Pandey and Nishchol Mishra. Phish-sight: a new approach for phishing detection using dominant colors on web pages and machine learning. *International Journal of Information Security*, pages 1–11, 2023.

[64] M E Pratiwi, T A Lorosae, and F W Wibowo. Phishing site detection analysis using artificial neural network. *Journal of Physics: Conference Series*, 1140(1):012048, dec 2018.

[65] T Rajendran, E Abishekraj, and U Dhanush. Improved intrusion detection system that uses machine learning techniques to proactively defend ddos attack. In *ITM Web of Conferences*, volume 56, page 05011. EDP Sciences, 2023.

[66] C Rajeswary and M Thirumaran. A comprehensive survey of automated website phishing detection techniques: A perspective of artificial intelligence and human behaviors. In *2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, pages 420–427. IEEE, 2023.

[67] Santhosh Raminedi, Trilok Nath Pandey, Venkat Amith Woonna, Sletzer Concy Mascarenhas, and Arjun Bharani. Classification of phishing websites using machine learning models. In *2023 3rd International conference on Artificial Intelligence and Signal Processing (AISP)*, pages 1–5. IEEE, 2023.

[68] Saba Hussein Rashid and Wisam Dawood Abdullah. Enhanced website phishing detection based on the cyber kill chain and cloud computing. *Indonesian Journal of Electrical Engineering and Computer Science*, 32(1):517–529, 2023.

[69] Jorge Enrique Rodr´ıguez Rodr´ıguez, V´ıctor Hugo Medina Garc´ıa, and Nelson Pérez Castillo. Webpages classification with phishing content using naive bayes algorithm. In *Knowledge Management in Organizations: 14th International Conference, KMO 2019, Zamora, Spain, July 15–18, 2019, Proceedings 14*, pages 249–258. Springer, 2019.

[70] Belyse Rugangazi and George Okeyo. Detecting phishing attacks using feature importance-based machine learning approach. In *2023 IEEE AFRICON*, pages 1–6. IEEE, 2023.

[71] Kishwar Sadaf. Phishing website detection using xgboost and catboost classifiers. In *2023 International Conference on Smart Computing and Application (ICSCA)*, pages 1–6. IEEE, 2023.

[72] Ozgur Koray Sahingoz, Ebubekir Buber, Onder Demir, and Banu Diri. Machine learning based phishing detection from urls. *Expert Systems with Applications*, 117:345–357, 2019.

[73] Said Salloum, Tarek Gaber, Sunil Vadera, and Khaled Shaalan. Phishing website detection from urls using classical machine learning ann model. In *International Conference on Security and Privacy in Communication Systems*, pages 509–523. Springer, 2021.

[74] Shafaizal Shabudin, Nor Samsiah Sani, Khairul Akram Zainal Ariffin, and Mohd Aliff. Feature selection for phishing website classification. *International Journal of Advanced Computer Science and Applications*, 11(4), 2020.

[75] Smita Sindhu, Sunil Parameshwar Patil, Arya Sreevalsan, Faiz Rahman, and Ms Saritha AN. Phishing detection using random forest, svm and neural network with backpropagation. In *2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)*, pages 391–394. IEEE, 2020.

[76] Daryle Smith, Sajad Khorsandroo, and Kaushik Roy. Supervised and unsupervised learning techniques utilizing malware datasets. In *2023 IEEE 2nd International Conference on AI in Cybersecurity (ICAIC)*, pages 1–7. IEEE, 2023.

[77] M Somesha, Alwyn Roshan Pais, Routhu Srinivasa Rao, and Vikram Singh Rathour. Efficient deep learning techniques for the detection of phishing websites. *Sādhanā*, 45:1–18, 2020.

[78] Gan Kim Soon, Chin Kim On, Nordaliela Mohd Rusli, Tan Soo Fun, Rayner Alfred, and Tan Tse Guan. Comparison of simple feedforward neural network, recurrent neural network and ensemble neural networks in phishing detection. In *Journal of Physics: Conference Series*, volume 1502, page 012033. IOP Publishing, 2020.

[79] Seun Mayowa Sunday. Phishing website detection using machine learning: Model development and django integration. *Journal of Electrical Engineering, Electronics, Control and Computer Science*, 9(3):39–54, 2023.

[80] Md Milon Uddin, Kazi Arfatul Islam, Muntasir Mamun, Vivek Kumar Tiwari, and Jounsup Park. A comparative analysis of machine learning-based website phishing detection using url information. In *2022 5th International Conference on Pattern Recognition and Artificial Intelligence (PRAI)*, pages 220–224. IEEE, 2022.

[81] Rambabu Vallepu and Malathi Karunakaran. An innovative method to improve performance analysis in classification with accuracy of phishing websites using random forest algorithm by comparing with support vector machine algorithm. In *AIP Conference Proceedings*, volume 2655. AIP Publishing, 2023.

[82] Xi-Zhao Wang, Yu-Lin He, and Debby D Wang. Non-naive bayesian classifiers for classification problems with continuous attributes. *IEEE transactions on cybernetics*, 44(1):21–39, 2013.
[83] Yifei Wang. A survey of phishing detection: from an intelligent countermeasures view. In *2022 IEEE Conference on Telecommunications, Optics and Computer Science (TOCS)*, pages 761–769. IEEE, 2022.
[84] Zhanfeng Wang, Lisha Yao, Xiaoyu Shao, and Honghai Wang. A combination of textcnn model and bayesian classifier for microblog sentiment analysis. *Journal of Combinatorial Optimization*, 45(4):109, 2023.
[85] Palla Yaswanth and V Nagaraju. Prediction of phishing sites in network using naive bayes compared over random forest with improved accuracy. In *2023 Eighth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*, pages 1–5. IEEE, 2023.
[86] Suleiman Y Yerima and Mohammed K Alzaylaee. High accuracy phishing detection based on convolutional neural networks. In *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)*, pages 1–6. IEEE, 2020.
[87] Qiao Zhang, Youjun Bu, Bo Chen, Surong Zhang, and Xiangyu Lu. Research on phishing webpage detection technology based on cnn-bilstm algorithm. *Journal of Physics: Conference Series*, 1738(1):012131, jan 2021.
[88] Erzhou Zhu, Yinyin Ju, Zhile Chen, Feng Liu, and Xianyong Fang. Dtof-ann: an artificial neural network phishing detection model based on decision tree and optimal features. *Applied Soft Computing*, 95:106505, 2020.
[89] Rasha Zieni, Luisa Massari, and Maria Carla Calzarossa. Phishing or not phishing? a survey on the detection of phishing websites. *IEEE Access*, 11:18499–18519, 2023.
[90] Ige, T., Marfo, W., Tonkinson, J., Adewale, S., & Matti, B. H. (2023). Adversarial sampling for fairness testing in deep neural network. arXiv preprint arXiv:2303.02874.
[91] Ige, Tosin, Christopher Kiekintveld, Aritran Piplai, Amy Wagler, Olukunle Kolade, and Bolanle Hafiz Matti. "An in-Depth Investigation Into the Performance of State-of-the-Art Zero-Shot, Single-Shot, and Few-Shot Learning Approaches on an Out-of-Distribution Zero-Day Malware Attack Detection." In 2024 International Symposium on Networks, Computers and Communications (ISNCC), pp. 1-6. IEEE, 2024.
[92] Ige, T., Kiekintveld, C., Piplai, A., Wagler, A., Kolade, O., & Matti, B. Ige, Tosin, Christopher Kiekintveld, Aritran Piplai, Amy Wagler, Olukunle Kolade, and Bolanle Hafiz Matti. "Towards an in-Depth Evaluation of the Performance, Suitability and Plausibility of Few-Shot Meta Transfer Learning on An Unknown Out-of-Distribution Cyber-attack Detection." In 2024 International Symposium on Networks, Computers and Communications (ISNCC), pp. 1-6. IEEE, 2024.
[93] Ige, T., Kiekintveld, C., & Piplai, A. (2024, May). An investigation into the performances of the state-of-the-art machine learning approaches for various cyber-attack detection: A survey. In 2024 IEEE International Conference on Electro Information Technology (eIT) (pp. 135-144). IEEE.
[94] Ige, T., Kiekintveld, C., & Piplai, A. (2024). Deep Learning-Based Speech and Vision Synthesis to Improve Phishing Attack Detection through a Multi-layer Adaptive Framework. arXiv preprint arXiv:2402.17249.
[95] Ogaga, D. and Abiodun Olalere. 2023 "Evaluation and Comparison of SVM, Deep Learning, and Naïve Bayes Performances for Natural Language Processing Text Classification Task" Preprints. https://doi.org/10.20944/preprints202311.1462.v1
[96] Abiodun Olalere , "Impact of Data Warehouse on Organization Development and Decision making (A Case study of United Bank for Africa and Watchlocker PLC) " International Journal of Research and Scientific Innovation (IJRSI) vol.10 issue 1, pp.36-45 January 2023 URL: https://www.rsisinternational.org/journals/ijrsi/digital-library/volume-10-issue-1/36-45.pdf
[97] Agboro, D. The Use of Machine Learning Methods for Image Classification in Medical Data. URL: https://philpapers.org/rec/AGBTUO
[98] Ogaga, Destiny and Zhao, Haoning, The Rise of Artificial Intelligence and Machine Learning in HealthCare Industry (May 15, 2023). International Journal of Research and Innovation in Applied Science , Available at SSRN: https://ssrn.com/abstract=4483867
[99] Destiny Ogaga, Haoning Zhao "The Rise of Artificial Intelligence and Machine Learning in HealthCare Industry " International Journal of Research and Innovation in Applied Science (IJRIAS) volume-8-issue-4, pp.250-253 April 2023 DOI: https://doi.org/10.51584/IJRIAS.2023.8426
[100] Ogaga, Destiny. "COURSE REGISTRATION AND EXAM PROCESSING SYSTEM." URL: https://www.researchgate.net/publication/374725473_COURSE_REGISTRATION_AND_EXAM_PROCESSING_SYSTEM