Computers, Materials & Continua
DOI: 10.32604/cmc.2023.036422
Article

Tech Science Press

Machine Learning Techniques for Detecting Phishing URL Attacks

Diana T. Mosa[1,2], Mahmoud Y. Shams[3,*], Amr A. Abohany[2], El-Sayed M. El-kenawy[4] and M. Thabet[5]

[1]Department of Cyber Security, College of Engineering and Information Technology, Buraydah Private Colleges, Buraydah, 51418, Kingdom of Saudi Arabia
[2]Faculty of Computers and Information, Kafrelsheikh University, Kafrelsheikh, 33516, Egypt
[3]Faculty of Artificial Intelligence, Kafrelsheikh University, Kafrelsheikh, 33516, Egypt
[4]Delta Higher Institute of Engineering and Technology, Mansoura, 35111, Egypt
[5]Faculty of Computers and Information, Fayoum University, Fayoum, Egypt
*Corresponding Author: Mahmoud Y. Shams. Email: mahmoud.yasin@ai.kfs.edu.eg
Received: 29 September 2022; Accepted: 09 December 2022

Abstract: Cyber Attacks are critical and destructive to all industry sectors. They affect social engineering by allowing unapproved access to a Personal Computer (PC) that breaks the corrupted system and threatens humans. The defense of security requires understanding the nature of Cyber Attacks, so prevention becomes easy and accurate by acquiring sufficient knowledge about various features of Cyber Attacks. Cyber-Security proposes appropriate actions that can handle and block attacks. A phishing attack is one of the cybercrimes in which users follow a link to illegal websites that will persuade them to divulge their private information. One of the online security challenges is the enormous number of daily transactions done via phishing sites. As Cyber-Security have a priority for all organizations, Cyber-Security risks are considered part of an organization's risk management process. This paper presents a survey of different modern machine-learning approaches that handle phishing problems and detect with high-quality accuracy different phishing attacks. A dataset consisting of more than 11000 websites from the Kaggle dataset was utilized and studying the effect of 30 website features and the resulting class label indicating whether or not it is a phishing website (1 or −1). Furthermore, we determined the confusion matrices of Machine Learning models: Neural Networks (NN), Naïve Bayes, and Adaboost, and the results indicated that the accuracies achieved were 90.23%, 92.97%, and 95.43%, respectively.

Keywords: Cyber security; phishing attack; URL phishing; online social networks; machine learning

1 Introduction

The internet is a wealthy source of social media applications [1]. Boyd et al. in 2007 proposed the definition of Online Social Networks (OSNs) [2]. OSNs applications varied from Mobile-Based and Web-Based that permit User-Generated content [3]. OSNs and Cyber-Physical systems are rapidly increasing. OSNs applications like LinkedIn, Pinterest, Whatsapp, Facebook, and Twitter are

important for communication with others via links with other members with common interests in the cloud despite thinking about geographical distances [4]. OSNs are not just for communication and continuous knowledge of the latest opinions and stories about any digital topic around the globe via the network [5]. In addition, they enhance E-Business by providing advertisements and promotions [6]. In recent years, a large number of Facebook attacks have been reported [7]. Irresponsible use of OSNs and ignorance of pinholes of phishing attacks cause constantly increasing attacks. Cybercriminals may attack users by getting their account information or contact phishing through spamming [8].

Cyber-Security is the standard used to block any attacks on systems [9]. Improving Cyber-Security and securing personal information have become one of the biggest challenges in the world. When the development of new web technologies like cloud computing, mobile computing, E-Commerce, net banking, etc., it is necessary to think about how to protect users. Governments think about "Cyber-Crimes" which are increasing in daily activities and creating attack pinholes for attackers to exploit [7,8]. Organizations interested in privacy and Cyber-Security are aware of their data and any new threats [4]. Despite the continuing effort of organizations to avoid Cyber-Security breaches and Cyber-Attacks, it is unavoidable because of successful attacks and their huge loss, and the effectiveness of Cyber-Security of networks becomes an essential issue. Ernst & Young reported that "Mobilization, virtualization, and cloud technology have created new technologies and opportunities in the business, making it more vulnerable to Cyber-Attacks" [10].

Recently, after the rise of the Internet of Things, the Cybercrime problem has increased greatly, which is considered a big challenge in the information technology field [9,11,12]. Cyber-Security protects organization assets against cybercriminals attack which may occur because of human error, planned attack, or the computer system limitation [10]. There is essential to identify malicious users when socializing over OSNs, as they may utilize camouflage and phishing techniques that cheat users into revealing their sensitive information [13]. There are many types of attacks used to acquire the personal information of people. As a result of the awareness lack, malicious content could be an executable, virus, javascript code, malware, adware, shell scripts, bat files, or set of commands via phishing sites, financial scams that trick people to buy products or take part in lucky events games [14].

In recent years, Internet users are insecure because of Web-Threats from social networks like social botnets. It is a collection of social users that convince users to release their personal information via malicious activities [15]. OSNs help in connecting people with similar interests and builds social relations. This leads to the availability of an enormous amount of users' information which attracts malicious users to open the way for criminals, perform undesired activities like phishing and identity theft, and begin attacks to access this information and violate the privacy of the users [5].

With the progress of network technology and the development of networking applications, security issues have become at risk. Phishing websites are capable of avoiding detection by looking legitimate which attracts these users to use these sites [16–19]. Phishing attacks are more and more complicated and make threats to people's network environments. The harm of phishing websites grows rapidly by increasing the number of fake messages which spread malicious information via visits to malicious Uniform Resource Locators (URLs) [14]. Organizations provide many social networking services to protect from these attacks by detecting phishing websites [16]. A chrome extension is a tool that can protect users from falling prey to malicious URLs activities [14].

Cyber-Security researchers and domain experts use Machine learning (ML) algorithms to build Anti-Phishing detectors models which can be applied in a Real-Time environment and interpret the results to defend against multimedia application attacks [20,21]. The major contribution of this study is listed as follows. Presenting a survey on the most common approaches utilized for detecting phishing attacks. Applying Machine Learning models NN, NB, and Adaboost to determine the accuracy,

sensitivity, precision, specificity, and F-score for the applied Kaggle dataset that represents URL phishing attacks.

The rest of the paper is structured as follows. Section 2 introduces social engineering and the life cycle of a social engineering attack. Section 3 describes social network attacks. The Anti-Phishing solutions are explained in Section 4. The Cyber-Security techniques to subdue attacks are introduced in Section 5. The limitation and threads are investigated in Section 6. Finally, the conclusion is given in Section 7.

2 Social Engineering

SE is a developed threat via different web applications. In the cyber domain, the human factor is more critical than the technical aspect. 95% of attacks are daily caused by human errors like providing personal information [22]. The attacks cause more and more economic losses. Mouton et al. have clarified SE as "The science of using social interaction have a way to convince others to respond with an attacker request" [5]. SE attacks are carried out in several phases with malicious activities as in Table 1.

Table 1: SE attacks phases with malicious activities

Phase	Activities of the attacker
Attack formulation	Identify goals and targets
Information gathering	Gather credibility information like preferences, affiliation, backgrounds, and social information to establish a trusting relationship
Planning	Analysis of collected information to develop an attack
Develop a relationship	The collected data is used to establish communication and build trust with the target
Exploit the relationship	Cheat the victim by a different wicked task, like logging in, spam email, password reset, and cloud access
Debrief	Received sensitive information used to access the cloud or system

Because of the rapid development of SE incidents, SE researchers confirm that there is no helpful defense method against these attacks [23]. Jamil et al. suggested a cycle framework for SE attacks [22]. The Life Cycle of a SE attack consists of six phases as described in Fig. 1.

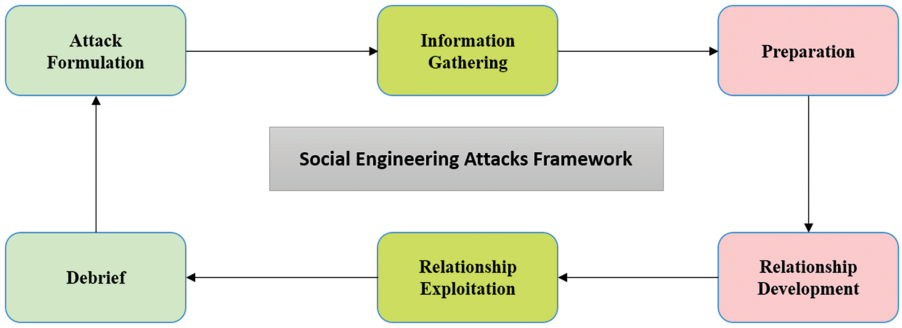

Figure 1: SE attacks life cycle

Traditional SE attacks, like phishing, do not require lots of knowledge to occur, so they are the reason for hundreds of millions in economic losses. Phishing attacks have globally increased by 1,220,523 in 2016 when compared with the preceding year. An appropriate SE framework contributes to the defense against SE attacks by illustrating the relationships between attack components [24].

3 Social Network Attacks

Cyber-Security is a critical issue in different industries as it causes enormous economic and reputation loss the in the majority of organizations [25]. In a cyberspace environment, through unapproved access to a PC, a threat uses words or images to steal sensitive information of others and produce serious damage by attacking different resources [26]. Limited knowledge of Cyber-Attacks features harmed victim organizations in all business sectors. The general social network Cyber-Attack and techniques in Cyber-Crimes have been identified in Table 2 [5].

Table 2: Main groups of social network attacks and techniques

Cyber-Attack	Techniques
Identity theft/Personal information	De-Anonymization Neighborhood Profile cloning Existing profile cloning Cross-Site profile cloning Social phishing attack
Spam	Simple spam attack Email-Based spam Broadcast spam Context-Aware HTTP session hijacking
Malware	Fake profile Social network API Drive-by download Shortened and hidden links Cross-Site scripting attack Click-Jacking

According to the Kaspersky Lab Global IT Risk Review, half of the business threats are cyber threats. Remote attacks increase Cyber-Attacks as they allow attackers to attack any PC anytime anywhere around the globe. RAKKSSA framework provides safety guidelines to reduce the risk of Cyber-Attacks and protect the organization's information. Cyber threat intelligence can provide a timely reply to attacks [10]. To secure the data processing for IoT middleware systems Ayoade et al. [27] presented an effective methodology to tackle the process of attacker authentication. Moreover, an architecture for developing crawling websites using DNN is presented by ElAraby et al. [28].

3.1 Social Networks Phishing Attacks

In social sites, a phishing attack is the most serious Cyber-Attack [5] that could cause destructive losses [26]. It is the most critical aspect of threats to internet security. As online daily transactions occur, much, this attack is Easy-to-Use on SE [29].

Phishing is a malicious technique for stealing others' data ethically and technically. Attackers contact people via different channels in social media [30]. Users drop into the trap of a phishing site, because of their ignorance enough knowledge about the URLs in security. As a result of the increasing reliance of individuals on cyberspace, the generation of digital information increases exponentially and the severity level of attack vectors increases continuously [26].

For the past two years, the Anti-Phishing working group detected about 97.36% of phishing websites. Security companies provide solutions for users to manage malicious activities. PhishMe develops software for organization security workers to deal with phishing attacks just by clicking on a button provided in the E-Mail client Add-in [31].

3.2 The Ecosystem of Phishing Attack Process

The ecosystem of the phishing attack process assumed that the victim receives a phishing email for instance with a fake link by the attacker and the attacker deals with a queue of phishing websites. These websites receive fake hosting and send sensitive data collection from the phasing dataset from the attackers. Mihai [32] suggest that the attack starts with showing a web service via a tricky HTTP form with a popular interface. This form contains a tricky link for the website, which the attacker hosts to collect the user's data. When the victim uses this link and interacts with the form by entering the required data, the data becomes under the control of the attacker [33] as clarified in Fig. 2.

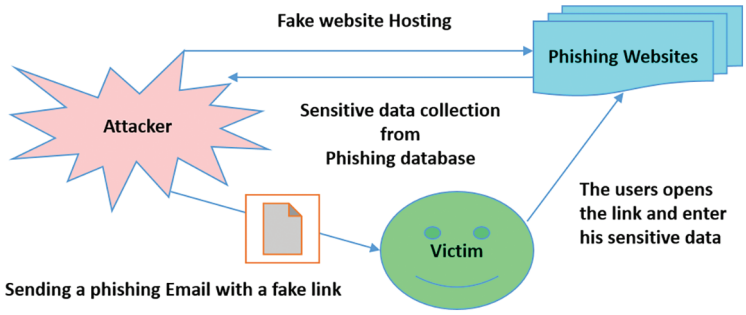

Figure 2: Traditional phishing process

3.3 Phishing Attacks Types

Spear Phishing (SP) is an attack that may be directed to steal the users' information from a specific company website. It is helpful by knocking towards intrusion in the system. While Clone Phishing (CP) is the attack here that depends on cheating victims by making an identical copy of the legal website in which the trap is made by attackers. Otherwise, Whaling Phishing (WP) is a Cyber-Attack similar to spear Phishing, but it targets High-Profiles [29,30].

4 Anti-Phishing Solutions

The detective technique is the most significant as it can reduce human errors by filtering and blocking access to phishing URLs that have installed kits. It is observable that using a combination

of hiding techniques may delay the detection of the site for up to ten hours. The preventive technique introduced by Well-Built authentication. A corrective technique introduced by like site removal [33].

4.1 Phishing Detective Technique Approaches

4.1.1 Software Grouping Approaches

This strategy distinguishes phishing and authentic sites by depending on programming devices that secure and differentiate attacks [34]. Table 3 shows different methodologies for phishing programming detection.

Table 3: Different software grouping approaches

Phishing programming detection methodologies			
Approaches	List-Based It is a list of harmful IP addresses, or Anti-Phishing toolbars (e.g. Google Safe Browsing API).	Heuristic-Based It depends on some URLs standards determined by cyber experts like lexical features, host and webpage information, etc.	Machine Learning-Based Discover phishing websites within given URLs via online learning which depends on several training classifiers.
Techniques	Whitelist-Based schemes	Phish-Guard Phish-Wish Visual similarity	Bag-of-Word Model-Based Methods Support Vector System K-Nearest neighbor Bart (Biayasian additive regression Tree) Neural networks
	Blacklist-Based schemes	Cantina Cantina+ Data mining	AdaBoost Decision tree Random forest algorithm Naïve bayes classifiers Boosting Logistic regression Bogus biter

4.1.2 User Preparing Approaches

These approaches depend on users' awareness and their ability to differentiate between phishing and authentic sites by improving their understanding of malicious assault [29].

4.2 Cyber Security Techniques to Subdue Attacks

To protect user accounts, researchers provide guidelines for securing accounts [35]. First, we used access control which is one of the basic cybersecurity measures in protecting information with a username and password. Second, data authentication, in which the antivirus's duty is to evaluate the validity of the incoming documents and decide whether their source is trustworthy or not. Finally, a firewall is software that examines whether messages are being entered or left online and filters those that do not satisfy security criteria, therefore assisting in the detection of hackers [36].

5 Discussion

Phishing is a deceptive attempt to get sensitive information in which attackers are always finding new ways to trick clients using social networking tactics by persuading them to follow instructions in a flow [37]. Anti-phishing Machine Learning (ML), Deep Learning (DL), scenario-based, and hybrid algorithms have all been created in recent years to detect phishing attacks, and they are continually improving. The finest outcomes come from machine learning approaches. DL and NLP techniques are quickly improving to track the URLs as text and to extract the character-level or word-level to feed DL models to identify the phishing URL websites. However, phishing website detection technologies continue to confront a number of challenges and limitations [38].

The Collection of URLs websites contains numerous validated phishing URLs, such as the phishtank-dot-com website, as an alternative. The drawback is that it necessitates an additional feature extraction process based on rules, and it is reliant on third-party services. This approach is independent of third-party services and unnecessary specialist knowledge; however, the learning process will take longer. It's simple to start using published datasets like the UCI machine learning dataset for the training process in academic articles, especially for complicated structured models like multi-layer neural networks [37]. Anti-phishing has been around for decades, and various efficient approaches have been developed. Attack techniques, on the other hand, are always developing, and no one-size-fits-all solution exists. It is worthwhile for us to continue investigating phishing website detection in order to protect against phishing attacks and minimise financial losses [38]. As indicated in Table 4, we compare various machine learning and deep learning models utilized by state-of-the-art studies in this part [39–60].

Table 4: Machine learning and deep learning models in state-of-the-art studies

Authors	Technique	Advantage	Disadvantage	Results obtained
(Gupta et al., 2021 [39])	Random forest	Without the usage of third-party services or the restricted attributes acquired from a URL, high accuracy and low response time were achieved.	There were no multiple datasets utilized to train the model, compare outcomes, or evaluate the model's resilience.	For 11964 instances of authentic and phishing URLs, the RF accuracy is 99.57%.

(Continued)

Table 4: Continued

Authors	Technique	Advantage	Disadvantage	Results obtained
(Sabahno et al., 2022 [40])	ISHO + SVM	The ISHO (improved spotted hyena optimization) technique has been improved to identify more efficient features.	A feature extraction process was not included in the proposed strategy.	They used SVM+ISHO with 98.64% accuracy using the UCI repository.
(Odeh et al., 2021 [41])	Adaboost	Weka 3.6, Python, and MATLAB 2 were employed in the suggested model.	There were no numerous datasets used to train the model, compare the findings, or assess the model's robustness.	A collection of different sites such as PhishTank, MillerSmiles, and Google searching archives, achieved 99.00% accuracy.
(Alsariera et al., 2020 [42])	Meta-learning algorithms and extra trees: LBET (logistic regression)	The accuracy is high, and the false-positive rate is minimal.	Additional methods to extract features and optimization strategies are required to boost the results obtained.	A collection of UCI repository websites is used to detect phishing attacks with 97.00% accuracy.
(Adeyemo et al., 2020 [43])	Bootstrap aggregating + logistic model tree	To reduce bias and variance, the classifiers were trained and evaluated using 10-fold cross-validation.	There is a lack of information about the way used to extract features.	UCI repository dataset is used and achieved 97.18% accuracy.

(Continued)

Table 4: Continued

Authors	Technique	Advantage	Disadvantage	Results obtained
(Zamir et al., 2020 [44])	Random forest + neural network + bagging	Focuses on detecting phishing websites using a feedforward NN and ensemble learners.	To verify its applicability in a real-time setting, the suggested approach may be integrated with alternative feature extraction models.	They used a dataset from the Kaggle website and achieved 97.4% accuracy.
(Wang et al., 2019 [45])	Recurrent neural network (RNN) + convolutional neural network (CNN)	The first to use a deep learning model to identify phishing in the context of cybersecurity concerns, as well as train and test with hundreds of thousands of phishing and non-phishing website URLs.	The training session was far too long. When the URL of the phishing website lacks crucial semantics, PDRCNN will be unable to classify effectively, regardless of whether the website matching the URL is active or has a problem.	A dataset including nearly 500,000 URLs gathered from Alexa and PhishTank obtained 97.00% accuracy.
(Aljofey et al., 2020 [46])	CNN	To compare the results of various sets of tests, four different groups of features are extracted.	The training time is extensive. The model is unconcerned with whether the URL of the website is active or includes an error. The algorithm will misclassify short links, sensitive terms, and phishing URLs that do not duplicate other websites.	They obtained 95.02% accuracy by collecting URLs from several sources (Alexa, openphish, spamhaus.org, tech-helplist.com, isc.sans.edu, and PhishTank).

(Continued)

Table 4: Continued

Authors	Technique	Advantage	Disadvantage	Results obtained
(Anupam et al., 2021 [47])	Grey wolf optimizer + SVM	Nature-inspired optimization methodologies, in addition to the grid search-optimized RF classifier, may be utilized to tune the parameters of the Support Vector Machine (SVM) model to achieve high accuracy.	Because the dataset is so small, there is no way to compare the findings of different datasets to the model.	The used UCI-ML repository dataset with an average accuracy reached 90%.
(Ali et al., 2019 [48])	Genetic algorithm (GA) + DNN	It's a novel concept to use GAs to pick effective characteristics and weights.	There isn't a way to extract features. Using GAs for feature selection and weighting may take longer. The detection accuracy may be reduced as compared to prior methodologies.	Using DNN, they obtained 93.34% accuracy. Out of 1353 websites in the UCI phishing websites dataset, there are 702 phishing websites, 548 legal websites, and 103 questionable websites.
(Deepa, 2021 [49])	Convolutional auto encoder + DNN	A convolutional autoencoder was used to extract features.	When compared to previous approaches, the detection accuracy may be lower. For deep learning models, the dataset is small.	They collect 16000 phishing and legitimate URLs. The phishing sites are made up of 12000 phishing URLs taken from PhishTank. They were also 89.00 % accuracy.

(Continued)

Table 4: Continued

Authors	Technique	Advantage	Disadvantage	Results obtained
(James et al., 2013 [50])	J48, JBK, SVM, NB	For analyzing numerous elements of benign and phishing URLs and detecting phishing websites, use lexical features, host attributes, and page priority properties and use fine-tuned parameters to separate the phishing sites from benign sites.	To constantly build new methods to fight defense measures, algorithms that react to new examples and features of phishing URLs are required.	A collection of URL websites from different resources are utilized with an average accuracy of 93.00%.
(Mao et al., 2018 [51])	SVM, RF, DT, AB	When it comes to detecting phishing pages, this tool is both accurate and robust. Create rules to determine the layout similarity of web pages and then detect phishing pages automatically. Phishtank.com provided over 2,900 phishing websites.	They should employ a prototyped strategy and test it against a huge number of phishing websites. Their technique has the potential to significantly improve the performance of existing antiphishing systems.	They compiled a list of phishing websites from phishtank.com. They verified and filtered such invalid pages first. They achieved an average 93.00% accuracy.

(Continued)

Table 4: Continued

Authors	Technique	Advantage	Disadvantage	Results obtained
(Buber et al., 2017 [52])	Decision Tree, Adaboost, K-star, kNN (n = 3), Random Forest, SMO and Naive Bayes, and different number/types of features as NLP based features, word vectors, and hybrid features.	The utilization of a significant number of phishing and genuine data, real-time execution, new website detection, independence from third-party services, and the use of feature-rich classifiers are all benefits. The Random Forest approach with solely NLP-based features has a 97.98 percent accuracy rate for phishing URL recognition.	Deep learning can be used to build the knowledge base to improve the system's efficiency.	Many tests were run on the proposed system, and the results indicated that the Random Forest algorithm attained 97.2 percent accuracy.
(Xiang et al., 2011 [53])	Feature-rich machine learning approach	Expand the number of features from their prior work to catch the continually evolving novel phishing attempts	8118 phishing pages and 4883 authentic web pages in a small dataset Take advantage of third-party services employ data about a certain location (top 100 English sites) 6 URL-based features, 4 HTML-based features, and 5 web-paged features	They achieved 92% accuracy based on the applied URL websites.

(Continued)

Table 4: Continued

Authors	Technique	Advantage	Disadvantage	Results obtained
(Le et al., 2011 [54])	Detects phishing websites by categorizing them using URL characteristics.	Based on an online classification, this product is suited for client-side deployment. tolerant of noisy data (training)	Using third-party services, we obtained a limited dataset (6083 malicious URLs and 8155 benign URLs).	They achieved 92.00% accuracy
(Jeeva et al., 2016 [55])	Algorithms for generating apriori and predicting apriori rules.	Rapid rule detection (particularly with apriori rules).	Make use of classification rules. Depending on how well the regulations are. 1200 phishing URLs and 200 authentic URLs in a restricted dataset 14 heuristic characteristics Nine apriori rules are a priori and nine predictive rules.	They obtained 93.00% accuracy.
(Babagoli et al., 2019 [56])	A nonlinear regression approach based on meta-heuristics and two feature selections.	The original UCI dataset has been reduced from 30 to 20, and decision trees will perform better with this feature set.	20 features are used in a restricted dataset (11055 phishing and authentic web pages).	The Harmony Search-based nonlinear regression yielded accuracy rates of 94.13% and 92.80% for the train and test procedures, respectively.
(Mohammad et al., 2014 [57])	Self-structuring neural networks with a type of artificial neural network.	In order to create network language independence, it employs an adaptive technique.	Third-party services (such as domain age) are utilized. a small sample size (1400 data). There are 17 features.	The major results indicated that the accuracy is 94.07% for 1000 Epochs.

(Continued)

Table 4: Continued

Authors	Technique	Advantage	Disadvantage	Results obtained
(Feng et al., 2018 [58])	Neural network with Monte Carlo algorithm	Not reliant on third parties. Real-time detection improves detection accuracy and consistency, as well as the ability to detect new phishing websites (zero-day attacks).	The use of third-party services necessary to obtain the whole page dataset is restricted (11055 data, 55.69 percent of which are phishing). 30 characteristics (address bar based, abnormal based, HTML and javascript based, domain based).	The use of third-party services necessary to obtain the whole page dataset is restricted (11055 data, 55.69 percent of which are phishing). 30 characteristics (address bar based, abnormal based, HTML and javascript based, domain based).
(Smadi et al., 2018 [59])	Neural network approach with reinforcement learning	Phishing emails were detected before the end-user saw them. Do not rely on real-time detection from third parties.	A limited sample size (9118 data, 50.0 percent of them are phishing). The 50 characteristics of PhishTank, 12 of which are URL-based, may be utilised to establish a blacklist.	The accuracy = 98.63%.

(Continued)

Table 4: Continued

Authors	Technique	Advantage	Disadvantage	Results obtained
(Peng et al., 2018 [60])	NLP and machine learning (using the Nave Bayes classifier).	Natural language processing is used to determine whether each sentence is suitable.	Based on the analysis of email text. A restricted dataset is utilized to create a blacklist of harmful pairs using machine learning (5009 phishing emails and 5000 legitimate emails).	The accuracy = 95%.

Machine learning models based on Neural Network (NN), Adaboost, and Naïve Bayes (NB) are utilized in this work to investigate the detection of phishing attacks using a dataset found on the Kaggle website "https://www.kaggle.com/code/maoryatskan/website-phishing-v2/data". The dataset is accessible in both text and CSV formats, and it includes the following resources that can be used as inputs for model construction: A database of website URLs for over 11000 websites. Each sample comprises 30 website parameters and a class label indicating whether or not it is a phishing website (1 or −1). The data collection is also used as input for project scoping, attempting to describe functional and non-functional needs. Fig. 3 and Table 5 show the results obtained representing the accuracy, precision, sensitivity, specificity, and F1-score of the proposed ML (NN, NB, and Adaboost) models [61,62].

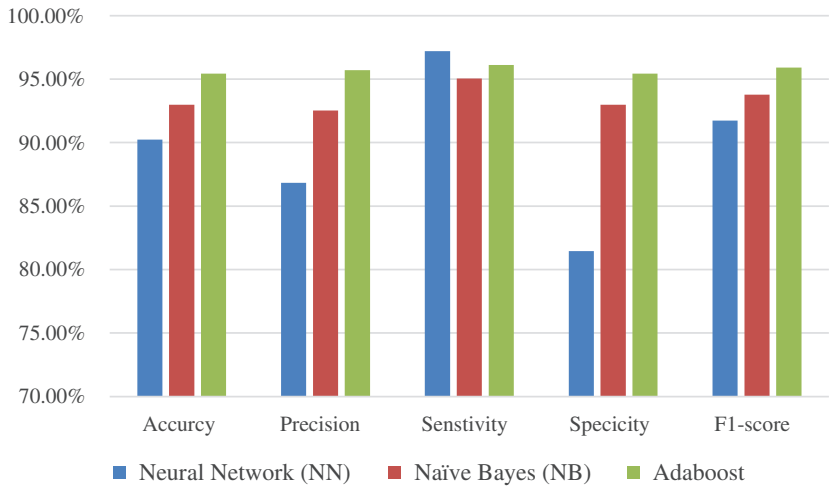

Figure 3: The results of the proposed ML (NN, NB, and Adaboost) models

Table 5: The confusion matrix results for the NN, NB, and Adaboost

	Neural Network (NN)	Naïve Bayes (NB)	Adaboost
Accuracy	90.23%	92.97%	95.43%
Precision	86.83%	92.54%	95.70%
Sensitivity	97.21%	95.05%	96.12%
Specificity	81.46%	92.97%	95.43%
F1-score	91.72%	93.77%	95.91%

6 Limitation

The major limitation of the current efforts to detect phishing attacks can be concluded in the following points. The preprocessing of data enrolled from the applied URL websites including imputation, and normalization should be performed before feature selection and extraction, especially for large-scale datasets. Due to the variability and change of URL information including the updated version, IP setting, or any other criteria. Therefore, the need to maintain and track the change should be simultaneously performed to tackle any new attacks and detect phishing attacks. In addition, the training period is lengthy. The model is indifferent whether the website's URL is active or contains an error. Short links, sensitive phrases, and phishing URLs that do not replicate other websites will be misclassified by the system.

7 Conclusion

Phishing is a serious security concern. It has a significant impact on the economic and online shopping sectors. Because online applications are a crucial interface for accessing and configuring user data, improper use of the web opens the door to targeted assaults by phishers who choose websites that are aesthetically and semantically identical to legitimate websites. Securing the online interface necessitates solutions that address dangers posed by both technological and social vulnerabilities. In the field of secure computing, preventing phishing attacks is a top goal and a serious difficulty. In this paper, we have presented comparative research for multiple classifiers to improve webpage security by detecting phishing websites by inspecting URLs. Machine learning techniques are a formidable defense and have a high learning capacity for making online message recipients aware of attacks and fraudulent websites. It can determine whether a website is safe or a phishing one. We can use detection approaches to check properties such as datasets, feature extraction and detection algorithms, and performance evaluation metrics as prevention tools. Attackers frequently overcome existing phishing defense methods based on URLs or page contents. The results of the paper investigated that the accuracy achieved was 90.23%, 92.97%, and 95.43% using NN, NB, and Adaboost ML models which indicates the reliability and robustness of the proposed method compared with the state-of-the-art methods.

Funding Statement: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Availability of Data and Materials: A data availability found at https://www.kaggle.com/code/maoryatskan/website-phishing-v2/data.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] D. Zeng, H. Chen, R. Lusch and S.-H. Li, "Social media analytics and intelligence," *IEEE Intelligent Systems*, vol. 25, no. 6, pp. 13–16, 2010.

[2] D. M. Boyd and N. B. Ellison, "Social network sites: Definition, history, and scholarship," *Journal of Computer-Mediated Communication*, vol. 13, no. 1, pp. 210–230, 2007.

[3] P. Ambika and M. B. Rajan, "Survey on diverse facets and research issues in social media mining," in *Int. Conf. on Research Advances in Integrated Navigation Systems (RAINS)*, Bangalore, India, pp. 1–6, 2016.

[4] D. Schlagwein and M. Hu, "How and why organisations use social media: Five use types and their relation to absorptive capacity," *Journal of Information Technology*, vol. 32, no. 2, pp. 194–209, 2017.

[5] K. Hameed and N. Rahman, "Today's social network sites: An analysis of emerging security risks and their counter measures," in *Int. Conf. on Communication Technologies (Com. Tech.)*, Rawalpindi, Pakistan, pp. 143–148, 2017.

[6] A. M. Kaplan and M. Haenlein, "Users of the world, unite! the challenges and opportunities of social media," *Business Horizons*, vol. 53, no. 1, pp. 59–68, 2010.

[7] R. M. Rodriguez and A. Atyabi, "Social engineering attacks and defenses in the physical world *vs.* cyberspace: A contrast study," Preprint ArXiv:2203.04813, pp. 1–26, 2022.

[8] M. K. Rogers, The psyche of cybercriminals: A psycho-social perspective. In: *Cybercrimes: A Multidisciplinary Analysis*. Berlin, Heidelberg: Springer, pp. 217–235, 2011.

[9] H. F. Atlam, A. Alenezi, M. O. Alassafi, A. A. Alshdadi and G. B. Wills, Security, cybercrime and digital forensics for IoT. In: *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, vol. 174, pp. 551–577, Intelligent Systems Reference Library: Cham, Switzerland, 2020.

[10] K. N. Zakaria, A. Zainal, S. H. Othman and M. N. Kassim, "Feature extraction and selection method of cyber-attack and threat profiling in cybersecurity audit," in *Int. Conf. on Cybersecurity (ICoCSec)*, Negeri Sembilan, Malaysia, pp. 1–6, 2019.

[11] A. Ali and W. Hussian, "Challenges and issues of the internet of things: Factoring elements from the social, political and information systems," in *Int. Conf. on Internet of Things as a Service, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, Sydney, Australia, vol. 421, pp. 73–83, 2022.

[12] M. K. Kagita, N. Thilakarathne, T. R. Gadekallu, P. K. R. Maddikunta and S. Singh, A review on cyber crimes on the internet of things. In: *Deep Learning for Security and Privacy Preservation in IoT*, 1st ed., Gateway East, Singapore: Springer, Signals and Communication Technology, pp. 83–98, 2021.

[13] J. Al-Muhtadi, A. Ranganathan, R. Campbell and M. D. Mickunas, "A flexible, privacy-preserving authentication framework for ubiquitous computing environments," in *Proc. 22nd Int. Conf. on Distributed Computing Systems Workshops*, Vienna, Austria, pp. 771–776, 2002.

[14] S. Shivangi, P. Debnath, K. Sajeevan and D. Annapurna, "Chrome extension for malicious URLs detection in social media applications using artificial neural networks and long short term memory networks," in *International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Bangalore, India, pp. 1993–1997, 2018.

[15] S. Abu-Nimeh, T. Chen and O. Alzubi, "Malicious and spam posts in online social networks," *Computer*, vol. 44, no. 9, pp. 23–28, 2011.

[16] T. Bilot, G. Geis and B. Hammi, "PhishGNN: A phishing website detection framework using graph neural networks," in *Proc. of the 19th Int. Conf. on Security and Cryptography - SECRYPT*, Lisbon, Portugal, pp. 428–435, 2022.

[17] J. Gu and H. Xu, "An ensemble method for phishing websites detection based on XGBoost," in *14th Int. Conf. on Computer Research and Development (ICCRD)*, Shenzhen, China, pp. 214–219, 2022.

[18] A. K. Jain and B. B. Gupta, "A survey of phishing attack techniques, defence mechanisms and open research challenges," *Enterprise Information Systems*, vol. 16, no. 4, pp. 527–565, 2022.
[19] N. Noah, A. Tayachew, S. Ryan and S. Das, "Phishercop: Developing an nlp-based automated tool for phishing detection," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 66, no. 1, pp. 2093–2097, 2022.
[20] K. Kumar and B. P. Pande, "Applications of machine learning techniques in the realm of cybersecurity," *Cyber Security and Digital Forensics*, vol. 1, no. 13, pp. 295–315, 2022.
[21] B. P. Kavin, S. Karki, S. Hemalatha, D. Singh, R. Vijayalakshmi *et al.,* "Machine learning-based secure data acquisition for fake accounts detection in future mobile communication networks," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, pp. 1–10, 2022.
[22] A. Jamil, K. Asif, Z. Ghulam, M. K. Nazir and S. M. Alam, "Mpmpa: A mitigation and prevention model for social engineering based phishing attacks on facebook," in *IEEE Int. Conf. on Big Data (Big Data)*, Seattle, WA, USA, pp. 5040–5048, 2018.
[23] K. Zheng, T. Wu, X. Wang, B. Wu and C. Wu, "A session and dialogue-based social engineering framework," *IEEE Access*, vol. 7, pp. 67781–67794, 2019.
[24] A. Sayghe, Y. Hu, I. Zografopoulos, X. Liu, R. G. Dutta *et al.,* "Survey of machine learning methods for detecting false data injection attacks in power systems," *IET Smart Grid*, vol. 3, no. 5, pp. 581–595, 2020.
[25] P. Rathod and T. Hämäläinen, "A novel model for cybersecurity economics and analysis," in *IEEE Int. Conf. on Computer and Information Technology (CIT)*, Helsinki, Finland, pp. 274–279, 2017.
[26] A. K. Jain and B. B. Gupta, PHISH-SAFE: URL features-based phishing detection system using machine learning. In: *Cyber Security, Advances in Intelligent Systems and Computing*. Vol. 729, pp. 467–474, 2018.
[27] G. Ayoade, A. El-Ghamry, V. Karande, L. Khan, M. Alrahmawy *et al.,* "Secure data processing for IoT middleware systems," *Journal of Supercomputing*, vol. 75, no. 8, pp. 4684–4709, 2019.
[28] M. E. ElAraby, S. M. Abuelenin, H. M. Moftah and M. Z. Rashad, "A new architecture for improving focused crawling using deep neural network," *Journal of Intelligent & Fuzzy Systems*, vol. 37, no. 1, pp. 1233–1245, 2019.
[29] M. V. Kunju, E. Dainel, H. C. Anthony and S. Bhelwa, "Evaluation of phishing techniques based on machine learning," in *2019 Int. Conf. on Intelligent Computing and Control Systems (ICCS)*, Madurai, India, pp. 963–968, 2019.
[30] D. N. Pande and P. S. Voditel, "Spear phishing: Diagnosing attack paradigm," in *Int. Conf. on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, India, pp. 2720–2724, 2017.
[31] C. Catal, G. Giray, B. Tekinerdogan, S. Kumar and S. Shukla, "Applications of deep learning for phishing detection: a systematic literature review," *Knowledge and Information Systems*, vol. 64, no. 6, pp. 1457–1500, 2022.
[32] I.-C. Mihai, "Management of eLearning platforms security," *E-Learning & Software for Education*, vol. 1, no. 12, pp. 1–6, 2016.
[33] C. Leite, J. J. Gondim, P. S. Barreto and E. A. Alchieri, "Waste flooding: A phishing retaliation tool," in *IEEE 18th Int. Symp. on Network Computing and Applications (NCA)*, Cambridge, MA, USA, pp. 1–8, 2019.
[34] Y. Huang, J. Qin and W. Wen, "Phishing URL detection via capsule-based neural network," in *IEEE 13th Int. Conf. on Anti-counterfeiting, Security, and Identification (ASID)*, Xiamen, China, pp. 22–26, 2019.
[35] J.Á. Concepción-Sánchez, J. Molina-Gil, P. Caballero-Gil and I. Santos-González, "Fuzzy logic system for identity theft detection in social networks," in *4th Int. Conf. on Big Data Innovations and Applications (Innovate-Data)*, Barcelona, Spain, pp. 65–70, 2018.
[36] G. N. Reddy and G. J. Reddy, "A study of cyber security challenges and its emerging trends on latest technologies," ArXiv Preprint:1402.1842, pp. 1–6, 2014.
[37] A. Basit, M. Zafar, X. Liu, A. R. Javed and Z. Jalil, "A comprehensive survey of AI-enabled phishing attacks detection techniques," *Telecommunication Systems*, vol. 76, no. 1, pp. 139–154, 2021.
[38] L. Tang and Q. H. Mahmoud, "A survey of machine learning-based solutions for phishing website detection," *Machine Learning and Knowledge Extraction*, vol. 3, no. 3, pp. 672–694, 2021.

[39] B. B. Gupta, K. Yadav, I. Razzak, K. Psannis, A. Castiglione *et al.,* "A novel approach for phishing URLs detection using lexical based machine learning in a real-time environment," *Computer Communications*, vol. 175, no. 3, pp. 47–57, 2021.
[40] M. Sabahno and F. Safara, "ISHO: Improved spotted hyena optimization algorithm for phishing website detection," *Multimedia Tools and Applications*, vol. 81, no. 1, pp. 34677–34696, 2022.
[41] A. Odeh, I. Keshta and E. Abdelfattah, "PHIBOOST-a novel phishing detection model using adaptive boosting approach," *Jordanian Journal of Computers and Information Technology (JJCIT)*, vol. 7, no. 1, pp. 64–73, 2021.
[42] Y. A. Alsariera, V. E. Adeyemo, A. O. Balogun and A. K. Alazzawi, "Ai meta-learners and extra-trees algorithm for the detection of phishing websites," *IEEE Access*, vol. 8, pp. 142532–142542, 2020.
[43] V. E. Adeyemo, A. O. Balogun, H. A. Mojeed, N. O. Akande and K. S. Adewole, "Ensemble-based logistic model trees for website phishing detection," in *Int. Conf. on Advances in Cyber Security*, Penang, Malaysia, pp. 627–641, 2020.
[44] A. Zamir, H. U. Khan, T. Iqbal, N. Yousaf, F. Aslam *et al.,* "Phishing web site detection using diverse machine learning algorithms," *The Electronic Library*, vol. 38, no. 1, pp. 65–80, 2020.
[45] W. Wang, F. Zhang, X. Luo and S. Zhang, "Pdrcnn: Precise phishing detection with recurrent convolutional neural networks," *Security and Communication Networks*, vol. 2019, no. 1, pp. 1–16, 2019.
[46] A. Aljofey, Q. Jiang, Q. Qu, M. Huang and J.-P. Niyigena, "An effective phishing detection model based on character level convolutional neural network from URL," *Electronics*, vol. 9, no. 1514, pp. 1–24, 2020.
[47] S. Anupam and A. K. Kar, "Phishing website detection using support vector machines and nature-inspired optimization algorithms," *Telecommunication Systems*, vol. 76, no. 1, pp. 17–32, 2021.
[48] W. Ali and A. A. Ahmed, "Hybrid intelligent phishing website prediction using deep neural networks with genetic algorithm-based feature selection and weighting," *IET Information Security*, vol. 13, no. 6, pp. 659–669, 2019.
[49] S. T. Deepa, "Phishing website detection using novel features and machine learning approach," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 7, pp. 2648–2653, 2021.
[50] J. James, L. Sandhya and C. Thomas, "Detection of phishing URLs using machine learning techniques," in *2013 Int. Conf. on Control Communication and Computing (ICCC)*, Thiruvananthapuram, India, pp. 304–309, 2013.
[51] J. Mao, J. Bian, W. Tian, S. Zhu, T. Wei *et al.,* "Detecting phishing websites via aggregation analysis of page layouts," *Procedia Computer Science*, vol. 129, no. 13, pp. 224–230, 2018.
[52] E. Buber, B. Diri and O. K. Sahingoz, "NLP based phishing attack detection from URLs," in *Int. Conf. on Intelligent Systems Design and Applications*, Delhi, India, pp. 608–618, 2017.
[53] G. Xiang, J. Hong, C. P. Rose and L. Cranor, "Cantina+ a feature-rich machine learning framework for detecting phishing web sites," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 2, pp. 1–28, 2011.
[54] A. Le, A. Markopoulou and M. Faloutsos, "PhishDef: URL names say it all," in *Proc. IEEE INFOCOM*, Shanghai, China, pp. 191–195, 2011.
[55] S. C. Jeeva and E. B. Rajsingh, "Intelligent phishing url detection using association rule mining," *Human-centric Computing and Information Sciences*, vol. 6, no. 1, pp. 1–19, 2016.
[56] M. Babagoli, M. P. Aghababa and V. Solouk, "Heuristic nonlinear regression strategy for detecting phishing websites," *Soft Computing*, vol. 23, no. 12, pp. 4315–4327, 2019.
[57] R. M. Mohammad, F. Thabtah and L. McCluskey, "Predicting phishing websites based on self-structuring neural network," *Neural Computing and Applications*, vol. 25, no. 2, pp. 443–458, 2014.
[58] F. Feng, Q. Zhou, Z. Shen, X. Yang, L. Han *et al.,* "The application of a novel neural network in the detection of phishing websites," *Journal of Ambient Intelligence and Humanized Computing*, vol. 2018, no. 13, pp. 1–15, 2018.
[59] S. Smadi, N. Aslam and L. Zhang, "Detection of online phishing email using dynamic evolving neural network based on reinforcement learning," *Decision Support Systems*, vol. 107, pp. 88–102, 2018.

[60] T. Peng, I. Harris and Y. Sawa, "Detecting phishing attacks using natural language processing and machine learning," in *2018 IEEE 12th Int. Conf. on Semantic Computing (ICSC)*, Laguna Hills, USA, pp. 300–301, 2018.

[61] A. Ibrahim, S. Mirjalili, M. El-Said, S. Ghoneim, M. Al-Harthi *et al.,* "Wind speed ensemble forecasting based on deep learning using adaptive dynamic optimization algorithm," *IEEE Access*, vol. 9, no. 1, pp. 125787–125804, 2021.

[62] A. Salamai, E.-S. M. El-kenawy and A. Ibrahim, "Dynamic voting classifier for risk identification in supply chain 4. 0," *Computers Materials & Continua*, vol. 69, no. 3, pp. 3749–3766, 2021.