Stochastic Modelling and Computational Sciences

PERFORMANCE ANALYSIS OF DIFFERENT MACHINE LEARNING TECHNIQUES FOR PHISHING WEBSITE DETECTION USING UNIFORM RESOURCE LOCATOR FEATURES

Er. Gurpreet Singh[1]
M-Tech Scholar, Yadavindra department of engineering, Punjabi University Guru Kashi Campus, Talwandi Sabo, Bathinda, Punjab

Dr. Rajbhupinder Kaur[2]
Assistant Professor in Computer Science and Engineering
Yadavindra department of engineering, Punjabi University Guru Kashi Campus, Talwandi Sabo, Bathinda, Punjab (Supervisor)

Dr. Manoj Kumar[3]
Assistant Professor in Computer Science and Engineering
Yadavindra department of engineering, Punjabi University Guru Kashi Campus, Talwandi Sabo, Bathinda, Punjab (Supervisor)

ABSTRACT
Phishing, a prevalent form of cyber fraud, exploits user trust to illicitly obtain sensitive information. Therefore, the detection of phishing attacks is considered crucial for ensuring online security. Over the years, various techniques are employed to detect phishing which include lists- based, visual similarity, heuristic, machine learning, and machine learning techniques. The present research used a novel data-set comprising 111 features extracted from 88,647 websites, differentiating between 30,647 instances labeled as phishing and 58,000 as legitimate by organizing data-set into six comprehensive categories viz. Uniform Resource Locator (URL), domain, directory, file, parameters, and resolving data and external metrics. The class imbalance was addressed using Synthetic Minority Over-sampling Technique (SMOTE) during analysis, and nine different machine learning classifiers viz. XGBoost, Random Forest (RF), Decision Tree (DT), AdaBoost, Logistic Regression (LR), Linear Discriminant Analysis (LDA), Stochastic Gradient Descent (SGD), k-Nearest Neighbor (KNN), and Naive Bayes were applied to assess performance. These results highlight that RF classifier has superior performance with high accuracy (98%), precision (0.98), recall (0.98), and F1-score (0.98), closely followed by the XGBoost classifier with almost equal accuracy (98%), precision (0.97), recall (0.98) and F1- score (0.98). Conversely, the SGD classifier has comparatively lower scores: accuracy (82%), precision (0.85), recall (0.76), and F1-score (0.84). Therefore, it is concluded that RF classifier was the most efficient machine learning technique for detecting phishing websites which outperforming other classifiers across accuracy, precision, recall, and F1-score metrics, and can highly contributes with valuable insights to the field of cyber security and aiding the development of robust phishing detection systems.

Keywords*: Phishing; preprocessing; feature selection; balancing; classification; machine learning; performance metrics*

INTRODUCTION
Phishing websites are fraudulent websites created with the intent to deceive users and trick them into providing sensitive information, such as login credentials, personal details, or financial information (FBI, 2022). These websites often imitate legitimate and trustworthy entities, such as banks, social media platforms, or online services, to appear authentic and lure users into disclosing confidential information (Kathrine et al., 2019). Phishing attacks are a type of cyber threat in which attackers employ deceptive tactics to trick individuals into divulging sensitive information, such as usernames, passwords, credit card details, or other personal data.

These attacks often exploit human psychology and use various techniques to create a false sense of trust and urgency (Kathrine et al., 2019; Naqvi et al., 2023). One prevalent attack leveraging human vulnerabilities has been the phishing attack, where the attacker manipulates the victim into performing actions that are detrimental to

both the victim and the system. Phishing, identified as a crime rooted in social engineering (Chen and Chen, 2019) has been defined by as a fraudulent attempt to present as a trusted entity with the aim of acquiring sensitive information (Sameen et al., 2020).

Security incidents and breaches aimed at exploiting the human aspects of cyber security are increasing annually (FBI, 2022). As per Data Breach Investigations Report (DBIR) by Verizon, ~82% of analyzed breaches involve a human element (Verizon, 2022). In recent times, phishing has targeted organizations, resulting in significant costs related to malware containment, productivity loss, credential compromise, and ransomware along with reputational damage (Ponemon Institute, 2021). Notably, phishing emerged as the costliest attack vector in 2022, averaging US$ ~4.91 million per data breach (IBM, 2022). Phishing can occur through various mediums and vectors which include the internet, short messaging services, and voice (Chiew et al., 2018). Recent trends indicate that phishing attempts have been observed across all sectors, ranging from financial institutions and educational organizations to government entities and the healthcare sector (IBM, 2022). Phishing is a form of cyber-criminal activity where a perpetrator, often a social engineer, deceives a target by posing as a trustworthy entity to extract sensitive information. In the context of internet-based phishing, this typically involves the use of emails or pop-ups that lead the target to a webpage resembling a legitimate site (Kathrine et al., 2019). On this deceptive page, users are prompted to enter their credentials under the guise of engaging in a fictitious scenario. Another phishing technique involves the distribution of deceptive emails, posing a risk as the attached files may harbor potential threats leading to data breaches—an undesirable event for both businesses and individuals (Kathrine et al., 2019; Ponemon Institute, 2021).

There are several techniques have been proposed for identifying phishing websites, including lists-based approaches, visual similarity analysis, heuristic methods and machine learning techniques (Zafar et al., 2021; Jain and Gupta, 2018). The browsers like Chrome, Firefox, and Explorer employ list-based approaches to identify phishing websites, and utilize

whitelists and blacklists. The whitelists consist of verified URLs that browsers can access, meaning only URLs present in the whitelist can be downloaded by the browser (Jain and Gupta, 2018). On the other hand, blacklists contain URLs associated with phishing or fraudulent activities, preventing browsers from accessing those web pages. However, list-based techniques have drawbacks, as a slight modification in the URL can bypass them, and the lists require frequent updates to counter new phishing URLs (Zafar et al., 2021). The visual similarity analysis approach evaluates suspected and legitimate websites based on various visual characteristics. By comparing textual content, text formatting, source code, webpage screenshots, website logos, images, and other visual elements, these methods identify similarities (Jain and Gupta, 2018). These visual similarity analysis techniques are limited as they compare the suspicious webpage to previously visited or saved pages and may not detect newly emerging phishing attempts (Zafar et al., 2021). The heuristic-based approach, on the other hand, utilizes features derived from phishing websites to distinguish them from legitimate ones based on various characteristics including URL, text content, digital certificates, website traffic, and Domain Name System (DNS) information (Jain and Gupta, 2018). The effectiveness of heuristic- based approaches depends on the feature set, training samples, and classification algorithms employed. Heuristic techniques can effectively detect zero-hour phishing attacks (Zafar et al., 2021). Similarly, machine learning techniques have gained popularity as an effective approach for phishing website detection (Catal et al., 2022; Naqvi et al., 2023). Initially, common features related to URLs, website structure, and JavaScript properties are collected to represent phishing URL and their associated websites (Catal et al., 2022). Phishing datasets are then compiled based on the selected features. Machine learning classifiers are trained using these datasets to identify phishing websites (Brereton et al., 2007; Naqvi et al., 2023). Machine learning techniques are particularly advantageous when dealing with large datasets with high velocity, variety, volume, value, and veracity (Catal et al., 2022). Machine learning classifiers have achieved accuracy rates exceeding 99%, making them highly effective (Naqvi et al., 2023).

After studying the relevant published literature related to the detection of phishing websites, it has been found that there is a need to develop accurate and efficient phishing detection systems that consistently provide good

accurate results. Although systems have been developed by various researchers in the past little work has been reported for phishing website detection with very good accuracy. The primary drawback of existing phishing detection systems

is their low accuracy. Additionally, researchers have often limited themselves to implementing their datasets on a small subset of machine learning models, without exploring the full range of applicable algorithms. Consequently, the proposed research work aims to address these aforementioned issues and develop a phishing detection system that can overcome these limitations. The present research was therefore conducted to (i) utilize a data-set that encompasses a larger number of instances of both phishing and legitimate URLs incorporating a broader range of features from phishing and legitimate websites into the data-set, (ii) enhance the accuracy of the phishing website detection system, and (iii) to analyze the selected data-set using various machine learning models.

PROPOSED METHODOLOGY

Data preprocessing and machine learning techniques

The process of phishing detection through URL features and machine learning algorithms involves multiple steps including data collection, data pre-processing, feature extraction, model training, model training and comparative analysis. The data was gathered from Mendeley data, an open-source online library, comprising 88,647 instances of URLs stored in a Comma- Separated Values (CSV) file (Vrbančič et al., 2020). The data-set comprises a diverse set of 111 distinct features, encompassing various aspects including properties derived from the URL, URL resolving metrics, and integration with external services. The data-set was partitioned into training and testing sub-sets. It was followed by the synthetic minority over-sampling technique (SMOTE) technique to preprocess and clean the data-set. The features were extracted from pre- processed data-set. Nine different machine learning models viz. XGBoost, Random Forest (RF), Decision Tree (DT), AdaBoost, Logistic Regression (LR), Linear Discriminant Analysis (LDA), Stochastic Gradient Descent (SGD), k-Nearest Neighbor (KNN), and Naive Bayes were developed and trained by using the training data (Babagoli et al., 2019; Garcés et al., 2019; Rao et al., 2020; Sánchez-Paniagua et al., 2021; Bashle and Gurta, 2022). The developed machine learning models were tested by using the testing data-set and employing different performance indices to establish the validity and verification of the models. The comparative analysis was performed based on accuracy to identify the superior performing model.

Among a total of 80647 instances, 30,647 instances were identified as phishing, while the remaining 58,000 instances were categorized as legitimate. This target attribute discerns the legitimacy of each instance, designated as either 0 for legitimate or 1 for phishing. To ensure data maturity and alignment with the intended format, the dataset underwent preprocessing. Subsequently, the data is partitioned into two training and testing data-set as 80:20. It means that 70% of the data is utilized as training data and 30% of the data is used as testing data-set. The 111 attributes within this meticulously prepared dataset are grouped into six distinct categories. The first grouping encapsulates features that span the entire URL string, while the subsequent four groupings delve into features specific to sub-strings. The final set of attributes is characterized by URL resolution metrics and external services integration, notably incorporating the Google search index (Vrbančič et al., 2020). For experimentation, the analysis and testing were executed within the Jupyter Notebook environment, hosted on a Windows 10 platform. The preprocessing method is the first step in preparing the data set for implementation. In this part, we cleaned the data by filling in missing values and removing noisy data (Vrbančič et al., 2020), and the attributes within the mentioned data-set were systematically categorized into six distinct groups. The pre-processed and balanced data-set divided into training and testing data sub-sets was used in machine learning models. After training the models, the test data-set was used to test the performance of the machine learning models.

PERFORMANCE APPRAISAL OF MACHINE LEARNING TECHNIQUES

The true positive (TP), false negative (FN), true negative (TN) and false positive (FP) values are given by the confusion matrix. This study uses binary classification for all models, in which ′1′ refers to a positive class, and ′0′ refers to a negative class. The probability of classifying a positive value as positive is known as TP and

classifying a positive value as negative is known as FN respectively. Similarly, the probability of classifying a negative value as negative is known as TN, and classifying a negative value as positive is known as FP respectively. Accuracy is regarded as the most important performance parameter to establish the performance of a prediction model. Accuracy quantifies the proportion of correct classifications (both TP and TN) concerning the total number of instances as calculated using Eq. 1 (Parikh et al., 2008).

$$\text{Accuracy} = (TP + TN) / (TP + TN + FP + FN) \quad (1)$$

Sensitivity reflects the percentage of accurate positive classifications (TP) out of truly positive instances. Sensitivity is the rate of occurrence of TPs and is defined as the probability of classifying the input positive data correctly and calculated using Eq. 2 (Parikh et al., 2008).

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

Specificity signifies the percentage of correctly classified positive records among all positive records. Specificity is the rate of occurrence of TNs and is calculated using Eq. 3 (Parikh et al., 2008).

$$\text{Specificity} = TN / (TN + FP) \quad (3)$$

Precision gauges the percentage of accurate positive classifications (TP) out of instances predicted as positive. The precision is the occurrence of TPs from a total positive occurrence which includes TPs and FPs and was calculated using Eq. 4 (Parikh et al., 2008).

$$\text{Precision} = TP / (TP + FP) \quad (4)$$

The F1-Measure quantifies the balanced harmonic mean of the test's precision and recall, providing a comprehensive evaluation of the model's performance. The F1 score was calculated using Eq. 5 (Parikh et al., 2008).

$$\text{F1-Measure} = 2 \times \text{Precision} \times \text{Recall} / (\text{Precision} + \text{Recall}) \quad (5)$$

These metrics collectively offer a comprehensive assessment of a classification model's effectiveness, capturing aspects such as accuracy, sensitivity, specificity, precision, and the balance between precision and recall through the F1-Measure.

RESULTS AND DISCUSSION

The efficacy of nine different machine learning models was assessed through comparative evaluation. These results culminate rigorous process which aids in determining the most adept model for the detection of phishing websites, thereby encapsulating the crux of the proposed dissertation work. The accuracy of the machine learning classifiers viz. XGBoost, RF, DT, AdaBoost, LR, LDASGD, KNN, and Naive Bayes varied between 82 and 98%, the highest for XGBoost and RF, whilst the lowest for Naive Bayes (Table 1). The precision value varied

between 0.85 and 0.98; the highest for XGBoost and RF classifiers, and the lowest value of 0.85 for Naïve Bayes and KNN classifier applied for phishing website detection. Based on precision value, these machine learning algorithms revealed relatively better performance of DT and AdaBost classifiers as compared to the LDA and SGD models. Similar to the accuracy and precision, the recall value was highest for XGBoost classifier, which was equal to that for RF model. It was observed that recall value ranged between 0.76 and 0.98. These results revealed that based on recall value, XGBoost and RF classifiers outperformed other classifiers. The lowest value of recall value of 0.76 illustrates the weak performance of Naïve Bayes classifier for phishing website detection. The F1-score attained a highest value of 0.98 for both XGBoosta nd RF classifiers, and the lowest for Naïve Bayes, whilst the others in-between. Kathrine et al., (2019) presented a framework for detecting and preventing various types of phishing attacks using machine learning based techniques and reported their outstanding performance in identifying TPs. They (Kathrine et al., 2019) further reported that only 14 research items did not cover deep learning techniques for mitigating phishing websites. In a survey-based study conducted by Basit et al., (2020) applied artificial intelligence in phishing detection techniques by evaluating anti-phishing techniques

into 16 machine learning, deep learning, hybrid learning, and scenario-based methods, with machine learning demonstrating superior results. The use machine, deep and hybrid AI-based learning techniques outperformed for phishing detection (Basit et al., 2020).

Similarly, Zafar et al., (2021) proposed a novel ensemble approach for detecting online phishing attacks using four machine learning classifiers viz. RF, artificial neural network (ANNs), KNN, and DT. By using data-set from the UCI repository which contains 11055 instances and 30 different features, the combination of KNN and RF classifier detects phishing attacks with 97.3% accuracy. However, Jain et al., (2018) applied a search engine-based technique using of TF-IDF to find the most relevant words of the website to use in the search query. The data-set was obtained from legitimate sites from Alexa and phishing sites from Open Phish and Phish Tank, and the system considered 200 sites for testing the accuracy and out of these 100 websites are legitimate sites and 100 sites are phishing. They (Jain et al., 2018) reported fairly satisfactory accuracy value of 89.0%, which was much lower as compared with the results of the present study. Sindhu et al., (2020) proposed a work that elaborates on the existing machine learning techniques used to detect phishing websites by implementing the improved RF classification method, Support Vector Machine (SVM) classification algorithm, and ANNS with back-propagation. The data-set they used in their study was obtained from the UCI Machine learning repository, which consisted 11,055 URLs with 6157 phishing samples and 4898 legitimate instances. Their results indicated high accuracy of 97.4, 97.5%, and 97.3% respectively with applied classifiers. However, the results of the present study highlight even higher accuracy value of 98% for both of XGBoost and RF classifiers. Jain et al., (2020) proposed a machine learning-based anti-phishing system to evaluate the performance of the system using 14 features from URLs to detect a website as phishing or non-phishing. The proposed system was trained using >33,000 phishing and legitimate URLs that are taken from PhishTank, and trained with SVM and Naive Bayes classifiers with ~91.3% accuracy in detecting phishing websites using the SVM classifier. In a different study, Al-Sariera et al., (2020) proposed four meta-learner models viz. AdaBoost-Extra Tree (ABET), Bagging-Extra tree (BET), Rotation Forest-Extra Tree (RoFBET) and LogitBoost-Extra Tree (LBET) using the extra-tree base classifier based on data-set available on the UCI and Kaggle websites, which consists of 11,055 instances and 30 independent attributes. They (Al-Sariera et al., 2020) reported that LBET model achieved detection accuracy >97.5%. Kumar et al., (2018) used several machine learning algorithms to train spam and phishing detectors by using CSDMC2010 spam corpus data-set which has ~2949 normal emails and 1378 spam emails. For phishing detection, the data-set was collected from the UCI machine learning repository, which has

11000 instances and 30 attributes using two algorithms viz. RF and multilayer perceptron. They (Kumar et al., 2018) reported that by applying a RF classifier, the model can detect spam and phishing emails with an accuracy of 89.2% and 97.7%, respectively. The proposed RF model was advised to be used for more detailed and complex data-sets for phishing detection. Hannousse and Yahiouche (2021) proposed a general strategy for constructing reproducible and expandable data-sets for phishing website detection by adopting an improved classification of phishing website features and picking a total of 87 well-known features to test the suggested model. The data-set used in this study was collected from various sources including Yandex, Alexa, Phishtank, and OpenPhish, which was subjected to different machine learning algorithms viz. SVM, DR, Naive Bayes, LR, and RF classifiers. Similar to the results of the present study, the highest accuracy score of 96.6% was achieved by using hybrid features and applying a RF classifier. Sahingoz et al., (2019) proposed a real-time anti-phishing system in this research which employs 7 different classification algorithms and natural language processing-based features viz. Naive Bayes, RF, KNN, AdaBoost, K-star, SMO and DT classifiers and reported that RF algorithm using only NLP-based characteristics has the best performance in detecting phishing URLs with a 98% accuracy rate. In a different study, Abedin et al., (2020) proposed a research work that includes three machine learning algorithms viz. KNN, LR, and RF to predict any website's phishing status. The models were trained using URL-based features to prevent zero- day attacks and the data-set used was gathered from Kaggle which contains 32 attributes 11504 instances. They (Abedin et al., 2020) reported that RF classifier performed with a precision of 97.0%, a recall of 99.0%, and F1-Score is 97.0%. Similar to previous research, the results of the present study corroborate the literature highlights showing superiority of RF classifier in phishing website detection.

Table 1. Performance indicators viz. accuracy, precision, recall and F1-score of different machine learning techniques for phishing website detection.

Machine Learning Model	Accuracy (%)	Precision	Recall	F1-score
XGBoost	98	0.98	0.98	0.98
Random Forest (RF)	98	0.97	0.98	0.98
Decision Tree (DT)	96	0.96	0.97	0.96
AdaBoost	94	0.95	0.97	0.94
Logistic Regression (LR)	92	0.93	0.96	0.92
Linear Discriminant Analysis (LDA)	91	0.92	0.96	0.91
Stochastic Gradient Descent (SGD)	91	0.92	0.92	0.91
K-Nearest Neighbour (KNN)	90	0.85	0.90	0.91
Naïve Bayes	82	0.85	0.76	0.84

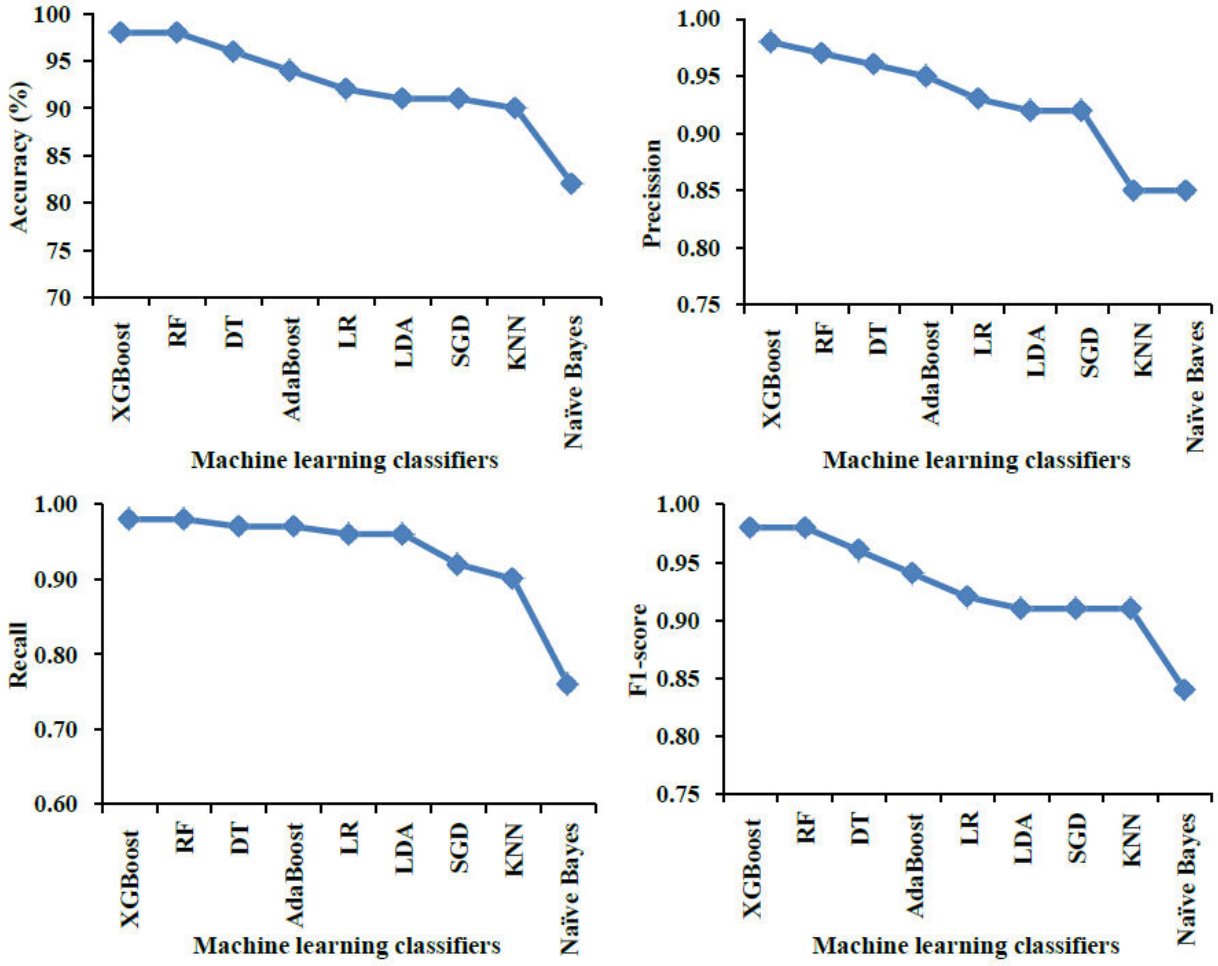

Figure 1. Performance evaluation of different machine learning classifiers viz. XGBoost, Random Forest (RF), Decision Tree (DT), AdaBoost, Logistic Regression (LR), Linear Discriminant Analysis (LDA), Stochastic Gradient Descent (SGD), k-Nearest Neighbor (KNN), and Naive Bayes applied for phishing website detection.

CONCLUSION

In addressing the challenge of detecting phishing websites using URL features through machine learning algorithms, this research utilized an open-source dataset comprising 111 informative URL features, encompassing 88,647 instances of both phishing and legitimate URLs. The study involved essential steps such as data cleaning, balancing, feature extraction, and partitioning into training (70.0%) and testing (30.0%) datasets. Employing ten diverse machine learning classifiers, including RF, XGBoost, DT, SGD, AdaBoost, LDA, KNN, LR, and Naive Bayes, the research evaluated and compared their performance using accuracy, precision, recall, and F1-score metrics. Experimental results underscore the effectiveness of this approach in achieving notable accuracy for phishing website URL detection. XGBoost emerged as the top- performing classifier, boasting an impressive accuracy of 91%, alongside precision, recall, and F1-score metrics, each at 91%. In contrast, the Naive Bayes classifier exhibited a lower accuracy of 83%, with precision, recall, and F1-score metrics at 91% each.

REFERENCES

A.K. Jain, B.B. Gupta. PHISH-SAFE: URL features-based phishing detection system using machine learning. Adv. Intell. Syst. Comput. 729: 467-474, 2018. doi:10.1007/978-981- 10-8536-9_44.

Abedin N.F., M. Saifuddin, R. Bawm, M.A. Rahman, T. Sarwar, S. Hossain. Phishing attack detection using machine learning classification techniques. Int. Conf. Intelli. Sustain. Syst. 1125-1130, 2020. doi:10.1109/ICISS49785.2020. 9315895

Al-Sariera Y.A., V.E. Adeyemo, A.O. Balogun, A.K. Alazzawi. AI meta-learners and extra-trees algorithm for the detection of phishing Websites. Access 8: 142532-142542, 2020. doi:10.1109/ACCESS.2020.3013699.

Babagoli M., M.P. Aghababa, V. Solouk. Heuristic nonlinear regression strategy for detecting phishing websites. Soft Comput. 23(12): 4315-4327, 2019. doi:10.1007/s00500-018-3084-2.

Bashle S., G. Gurta. Performance evaluation of various classification techniques for customer churn prediction in e-commerce. Microprocessors and Microsystems 94: 1-19, 2022. doi: 10.1016/j.micpro.2022.104680.

Basit A, M. Zafar, A.R. Javed, Z. Jalil. A novel ensemble machine learning method to detect phishing attack. Int. Multi-Topic Conf. 1-5, 2020. doi:10.1109/INMIC50486.2020.9318210

Brereton, P., Kitchenham, B.A., Budgen, D., Turner, M., Khalil, M., 2007. Lessons from applying the systematic literature review process within the software engineering domain. J. Syst. Softw. 80 (4), 571–583.

Catal, C., Giray, G., Tekinerdogan, B., Kumar, S., Shukla, S., 2022. Applications of deep learning for phishing detection: a systematic literature review. Knowl. Inf. Syst. 64 (6), 1457–1500.

Chen, Y.-H., Chen, J.-L., 2019. AI@ntiPhish — Machine Learning Mechanisms for Cyber- Phishing Attack. IEICE. Trans. Inf. Syst. E102.D (5), 878–887. doi:10.1587/ transinf.2018NTI0001.

Chiew, K.L., Yong, K.L.C, Tan, C.L., 2018. A survey of phishing attacks: their types, vectors, and technical approaches. Expert Syst. Appl. 106 (2018), 1–20.

FBI, "FBI releases the Internet Crime Complaint Center 2022 Internet crime report, including COVID-19 scam statistics," Available at: https://www.fbi.gov/contact-us/field- offices/springfield/news/internet-crimecomplaint-center-releases-2022-statistics, 2023G.

Garcés I.O., M. F. Cazares and R. O. Andrade. Detection of phishing attacks with machine learning techniques in cognitive security architecture. Int. Conf. Comput. Sci. & Comput. Intelli. 366-370, 2019. doi:10.1109/CSCI49370. 2019.00071.

Hannousse A, S. Yahiouche. Towards benchmark datasets for machine learning based website phishing detection: An experimental study. Engg. Appl. Arti. Intelli. 104: 1-17, 2021. doi:10.1016/j.engappai.2021.104347.

Jain A.K., B.B. Gupta. PHISH-SAFE: URL features-based phishing detection system using machine learning. Adv. Intell. Syst. Comput. 729: 467-474, 2018. doi:10.1007/978-981- 10-8536-9_44.

Jain A.K., S. Parashar, P. Katare, I. Sharma. PhishSKaPe: A Content based Approach to Escape Phishing Attacks. Procedia Comput. Sci. 171: 1102-1109, 2020. doi:10.1016/j.procs.2020.04.118.

Kathrine J.W., A.A. Rose, P.M. Praise, E.C. Kalaivani. Variants of phishing attacks and their detection techniques. Int. Conf. Trends in Electro. Inform. 255-259, 2019. doi: 10.1109/ICOEI.2019.8862697.

Naqvi B, Kseniia Perova, Ali Farooq, Imran Makhdoom, Shola Oyedeji, Jari Porras (2023) Mitigation strategies against the phishing attacks: A systematic literature review, Computers & Security, 132; 103387. https://doi.org/10.1016/j.cose.2023.103387.

Parikh R., A. Mathai, S. Parikh, G.C. Sekhar, R. Thomas. Understanding and using sensitivity, specificity, and predictive values. Indian Journal of Ophthalmology, 56(1): 45-50, 2008. doi:10.4103/0301-4738.3759

Ponemon Institute. (2021). The 2021 Cost of Phishing Study. Available at: https://www.proofpoint.com/sites/default/files/analyst-reports/pfpt-us-ar-ponemon2021-cost- of-phishing-study.pdf.

Rao R.S., T. Vaishnavi, A.R. Pais. Catch Phish: Detection of phishing websites by inspecting URL. J. Amb. Intelli. Human Comput. 11(2): 813-825, 2020. doi:10.1007/s12652-019- 01311-4.

S. Kumar, A. Faizan, A. Viinikainen, T. Hamalainen. MLSPD – Machine learning based spam and phishing detection. Lect. Notes Comput. Sci., Lect. Notes in Artif. Intelli. & Lect. Notes in Bioinfor. Springer: 510-522, 2018.

Sahingoz O.K., E. Buber, O. Demir, B. Diri. Machine learning based phishing detection from URLs. Expert Syst. Appl. 117: 345-357, 2019. doi:10.1016/j.eswa.2018.09.029.

Sameen, M., Han, K., Hwang, S.O., 2020. PhishHaven—an Efficient Real-Time AI Phishing URLs Detection System. IEEE Access 8, 83425–83443. doi:10.1109/ ACCESS.2020.2991403

Sánchez-Paniagua M., E. Fidalgo, V. González-Castro, E. Alegre. Impact of current phishing strategies in machine learning models for phishing detection. Adv. Intell. Syst. Comput. 1267: 87-96, 2021. doi:10.1007/978-3-030-57805-3_9.

Sindhu S., S.P. Patil, A. Sreevalsan, F. Rahman, A.N. Saritha. Phishing detection using random forest, SVM and neural network with backpropagation. Int. Conf. Smart Tech. Comput. Elect. Electro, 2020. doi:10.1109/ICSTCEE49637.2020. 9277256.

Verizon. (2022). Data Breach Investigations Report (DBIR). Available at: https://www.verizon.com/business/resources/T920/reports/dbir/2022-databreach- investigations-report-dbir.pdf.

Vrbančič G., I. Fister Jr., V. Podgorelec. Datasets for phishing websites detection. Data Brief 33: 1-7, 2020. doi:10.1016/j.dib.2020.106438.

Zafar M., X. Liu, A.R. Javed, Z. Jalil, K. Kifayat. A comprehensive survey of AIenabled phishing attacks detection techniques," Telecom. Syst. 76(1): 139-154, 2021. doi:10.1007/s11235-020-00733-2.