2024 آب العدد 14
No.14 Aug 2024
المجلة العراقية للبحوث الإنسانية والإجتماعية والعلمية
Iraqi Journal of Humanitarian, Social and Scientific Research
Print ISSN 2710-0952 Electronic ISSN 2790-1254

طريقة جديدة لتحديد الميزات عن طريق التحسين لزيادة دقة اكتشاف مواقع التصيد الاحتيالي

مسلم موسى سعيد
جامعة قم
كلية الهندسة والتكنولوجيا

خلاصة

لا تزال حماية الويب تمثل مشكلة خطيرة بسبب هجمات التصيد الاحتيالي، والتي تؤثر بدورها أيضا على الامن السيبراني وبالتالي الحاجة إلى أنظمة كشف قوية. في هذا البحث، تم اقتراح أسلوب جديد في اختيار الميزات عن طريق طريقة التحسين لزيادة دقة اكتشاف مواقع التصيد الاحتيالي. تتضمن الإستراتيجية اختيار وتصنيف السمات المميزة المفيدة، ويتفوق النهج المقترح على الأساليب الأساسية التقليدية في مجموعة من مقاييس التقييم عن طريق الاختيار المنهجي وتصنيف الميزات ذات الصلة تحت توجيه تقنيات التحسين المتطورة، ويتفوق في نتائجه على الطرق التقليدية، وبالتالي، هناك حاجة إلى تعزيز أنظمة الكشف الجيدة، والتي يجب أن تكون حاسمة للغاية مرة أخرى، من أجل تقليل الهجمات، إن لم يكن القضاء عليها، مثل تلك المتعلقة بالتصيد الاحتيالي. ويرجع ذلك إلى إمكانية تطبيقها بشكل عام، وإمكانية تكييف الطريقة مع العديد من المشاكل المختلفة، وإمكانية موازنتها، مما يجعلها سريعة نسبيًا مع عدد منخفض نسبيًا من الإيجابيات والسلبيات الكاذبة. الأعمال المستقبلية المطلوب القيام بها هي كما يلي: في المستقبل، يجب تجربة دمج نماذج التعلم الآلي وإجراء تجارب اختبار واقعية في الوقت الفعلي للطريقة المحددة لتقييم جدواها وإمكانية تطبيقها.

الكلمات المفتاحية: الأمن السيبراني، اختيار الميزات، طريقة التحسين، والكشف عن مواقع التصيد الاحتيالي، ومقاييس التقييم، والتعلم الآلي (ML).

A New Method for Feature Selection by Optimization for increase the Phishing Website Detection Accuracy

Muslim Mousa Saeed
muslimsa3eed@gmail.com
University of Qom -Engineering and Technical Faculty

Abstract

Web protection is still a serious problem due to phishing attacks which in turn also affects cybersecurity, therefore the need for strong detection systems. In this paper, a new approach in the feature selection by optimization method is proposed for increase detecting phishing websites accuracy. The strategy includes selection and ranking of beneficial characteristic features selection , The suggested approach beats conventional baseline methods on a range of evaluation metrics by methodically choosing and ranking pertinent features under the guidance of sophisticated optimization techniques, In their results that it outperforms traditional methods when measured against different methods, Thus, the need to enhance the good detection systems, which should be very crucial once again, in order to minimize if not eliminate the attacks, such as those related to phishing. This is due to its general applicability, the possibility to adapt the method to many classes of problems, and the possibility to parallelize it, which makes it relatively fast with a relatively low number of false positives and false negatives. The future works that are required to be done are as follows: In future, incorporation of

machine learning models has to be tried and real time field test experiments for the given method to assess its feasibility and applicability.

Keywords: Cyber-security, feature selection, optimization method, phishing website detection, evaluation metrics, machine learning (ML).

- **Introduction**

Cybersquatters have increased their numbers and are a menace to anyone who ends up on the fake sites, be it an individual, organization, or other kind of entity. In essence, such a fraudulent site works based on certain guidelines that include cheating the user and making the latter provide passwords to his or her login, the details of the user's account, and other aspects of his or her personal life [1]. These findings can culminate into identity theft, loss of money, damaging a business's reputation, and customers' disruption with large-scale effects. The prevention of the presented risks, which are inherent in phishing attacks, can only be prevented by using efficient examination systems. But traditional methodologies that solely focus on signatures or even heuristic patterns have not proved to be strong enough to meet the growing trends in the techniques used by the adversaries [1].

In an attempt to enhance the means currently employed in present day to detect the fake websites, which is the creations of the phisher, feature selection approaches are used [2].

Feature selection or feature extraction focuses on the effort to differentiate between the feature of the phishing site and the real site and does not take care of, the difference between the real site and the phishing site in order to avoid false positive mistakes. It also insisted on enhancing the method used in detecting the drug that has led to the recent enhancement. These distinguishing characteristics can be divided into the following: Modifications made: spatial changes: user behavior pattern, other content: structures, landing page, and URLs parameter characteristics. These statistics suggest that over the last decade, there have been significant advances and various feature selection techniques; however, new problems arise. Some of the conventional approaches disregard high characteristic factors and fail to consider checks which are performed on detection accuracy [2].

The main purpose of this study is to address the aforementioned problem and offer an optimization-based method to enhance the detection of phishing websites. Thus, essential challenges can be resolved using state-of-art models for optimization, and choose the most suitable distinctive features avoiding interferences that are noise and dimensionality [3]. It is for this reason that we see the necessity for better and more functional systems for phishing detection, which motivates us to create this project. Feature selection in the context of phishing

detection is given a scientific approach and it is built on a new approach to defining feature selection that differs from heuristic approaches [3].

However, it is needful to build a real time experiment to demonstrate that the new technique generates superior or at least enhanced results to the testbed vs and outcome enhanced than the baseline techniques. To all these outcomes the following paper proposes way for diagnosis of phishing web sites using feature selection which will complement other existing methodology in security against increase in phishing.

For this reason, the enhancement takes in a more accurate figure in the detection rate and existence to preclude users and firms from the risk of such an attack.

- **Literature Review**

It will also be useful now to see the prior studies that have been applied to phishing sites

1 -Signature-Based Detection: incorporates signatures or pattern known phishing websites to identify and prevent suspicious URLs and emails

2 -Heuristic Analysis: engages a fixed set of rules and algorithms to screen users behavior, Domain attributes, and the contents of Web sites.[4]

3 -Blacklist-Whitelist: maintains two lists that consist of sites it has recognized to be a threat and safe sites to classify and filter incoming web traffic

4-ML (Machine Learning): It is by these means that classifiers are classified through the application of the Machine learning algorithms that utilize feature extracted from phishing and genuine websites [4] .

5 -URL Analysis: concentrates on the parsing of URLs in order to detect features that seem suspicious and may hint at phishing relying on the structure, syntax and the properties of the URLs.

6 -Web Content Analysis: searches for a presence of phishing in the content of a website and tries to imitate the presence of phishing with the help of such elements as fakes, logos, and suspicious language.

7- Behavior-Based Detection: monitors several events that a user does on the website, including form submissions and redirects, primarily to analyze for novel activity that may be considered a phishing attempt.

The use of features in phishing detection techniques greatly improves their efficiency and accuracy. In this article, we examine some of the current feature selection methods.

-Filters

These methods ascertain the significance of a single feature without using the classification algorithm. Using CFS, Chi-square and Information Gain are a few norms.

CFS (Correlation based Feature Selection): is an algorithm that uses this evaluation formula in conjunction with a heuristic search method and an acceptable correlation measure.

Chi-Square test: is frequently applied while choosing features. Determining which features are most pertinent to the predictions task is the aim of feature selection. If there is a substantial correlation between each attribute and the targe, it can be found using the Chi-Square test [5].

Entropy: If classification is utilized, it is important to lower entropy since it reduces uncertainty and makes it possible to obtain new information.

-Wrappers

Of the different wrapper methods, a specific learning algorithm concealed behind a black box is implemented to evaluate the feature subsets. When the classifier is additionally used, they choose the feature subsets that yield verified results [6]. When using Forward Selections, the most pertinent features are added first, till performance continues to improve, and then the empty feature set is submitted. Genetic Algorithms: which, to simulate evolution, represent solution as chromosomes and subsequently evolve them via recombinant processes, mutations, and selection are most effectively used to find ideal feature subsets.

-the Methods of Embedded

With the embedded approach, the feature selection feature is always integrated into the model generation process itself. In the course of training the model, they obstruct the process of creating and executing the feature selection procedure. An additional effort is placed on a diver during a diving operation in order to mimic the responsibilities performed by an underwater welder.

With the combination of Lasso and Ridge regularization penalties, Elastic Net is a model that simultaneously generates selection of features and model regularization [6].

The degree to which a feature lowers impurity or mistake in decision trees inside a Random Forest model is indicated by its importance in the Random Forest model.

Hybrid Methodologies

In order to attain high accuracy, many scientists mix various procedures or consult domain-specific information by hybridizing diverse feature selection strategies.

1-One of the most important phases in phishing site detection systems that perform poorly due to conditional sensitivity of the data input property is feature selection. New studies test out novel approaches [7].

2-Gaussian Process Using the Gaussian process (GP) is one method since it at capturing the latent relevance between the input and output attributes.

3-EMO Algorithms for multiobjective feature selection, aim to strike a compromise between the complexity of many optimization goals. Among them is maximizing classification performance while decreasing the number of specified characteristics. [7].

Constraints and difficulties with the present approaches

The effectiveness and dependability of current methods are hampered by a number of constraints and obstacles that remain despite breakthroughs in detection of phishing websites techniques:

1-Evolution of Phishing Methods such as: Phishing is still a problem today because it takes on increasingly sophisticated and sly forms that employ cutting-edge methods to evade detection. Conventional methods of operation that rely on pre-established rules or fixed signatures will not succeed [7].

2-Zero-Day Attacks: These result in issues with systems that detect things. The attacks might not have been obvious until we signed our knowing prices, thus damage might have already been done after discretion.

3-Unbalanced Datasets: The majority of the time, the predicted problem dataset for identifying phishing websites has a skewed distribution since a large number of the websites are genuine rather than phishing [8].

4-Redundancy and Irrelevance of Features: The majority of features currently used by classifiers for detection of phishing contain redundant or irrelevant information, which can impair model performance and increase computational costs. Because some features are more visually appealing and important than others, selecting features is a continual challenge [8].

5-High-Dimensionality: Certain features may be unnecessary or redundant in issues involving high-dimensional feature spaces. For maximum effectiveness, these unnecessary or duplicated features must be removed. A significant research problem for identifying intrusion data as normal or invasive is effective feature selection [9].

6-Scalability: Scalability can be a problem, particularly for real-time systems that must handle massive web traffic volumes in a brief amount of time. The computational difficulty of the techniques for selecting features and the

requirement for constant updating of the systems for detection may be the reason of these challenges' rather broad scope.

Analysis of the gaps that led to the suggested Optimization Driven Feature:

In addition to highlighting the potential advantages of an optimization-driven strategy, a gap analysis identifies many critical areas where existing methodologies are deficient.

1-Feature Selection Optimization: Currently available feature extraction algorithms lack the accuracy in expressing data in high-dimensional features and the power to recognize URLs to phishing sites [9]. Researchers can quickly and efficiently identify a solution space by utilizing the suggested method, which also makes it easier to concentrate on crucial aspects while ignoring less significant ones.

2- Flexibility Against Changing Dangers: Due to their adaptability and frequent updating, phishing attacks should be monitored using visual systems capable of automatically evolving in a similar way [9]. The optimization-based technique incorporates adaptive dynamics, meaning that dynamic optimization algorithms are used to account for changes in the hazard environment and that models are updated on a regular basis to improve detection.

3- Accuracy and Efficiency (Striking a Balance): Maintaining optimal levels of accuracy and efficiency while striking a balance is necessary to get the greatest results from the recommended technique.

4- Combining Various Criteria: Reducing complexity, minimizing false positives, and improving detection accuracy are the three main challenges associated with phishing detection [10].

The suggested optimization-based approach will be able to provide the best results in identifying phishing sites and will resolve weak points by incorporating contemporary feature selection approaches [10]. With the aim of pushing the state of the art, the suggested approach progressively investigates the feature space and explains the optimization procedure for multi-purpose detection models.

- **Methodology**

A. Summary of Method for Feature Selection by Optimization

Improving the speed and accuracy of identifying fraudulent websites while also classifying related features while accounting for feature dimensionality and noise is the primary objective of optimizing the feature selection approach. The proposed approach Combining optimization techniques with the algorithms employed in this [11].

The fundamental concept is to find an ideal subset of attributes that improve the ability to distinguish between reputable and phishing websites using optimization methods, therefore increasing the accuracy of the classifier. The method finds the finest characteristic components for categorization by effectively navigating the feature space [11].

B. An explanation of the optimization methods employed

The feature selection method makes use of several optimization techniques, like as

1-Genetic Algorithms (GA): GA manages a population of potential approaches represented as chromosomes, drawing inspiration from natural selection and evolution. To produce new offspring solutions, it uses processes of crossover, mutation, and selection.

2- Particle swarm optimizing (PSO): PSO imitates fish schools and flocking of birds. Particles that represent potential solutions move according to both their own positions and the optimal positions of the swarm.

3- Ant colonial optimization (ACO): ACO uses pheromone trails that are repeatedly deposited on a graph that represents the search space in order to construct solutions by imitating the foraging behavior of ants.

C. Selection of Features Methods and Evaluation Metrics Explained

Selection criteria like the following are used in the feature selection process:

Information Gained: Measure the reductions in ambiguity whenever a particular attribute is given, helping Classification decision-making.

Chi-square Test: Ascertains correlations between characteristics and categories; qualities that are more distinct are indicated by higher $\chi 2$ values.

Mutual Information: A measure of the amount of information that a feature and class labels exchange, giving larger mutual information values to features in order of priority[12].

By accounting for the decrease in false positive alerts, the metrics assess the efficacy and efficiency of the system employed to detect phishing sites.These measures includes precision, accuracy, and AUC-ROC curve values.

D. Detailed Algorithmic Procedures for the Suggested Method

1.Initialization: Use randomly chosen features for starting the population of possible feature subsets.

2.Evaluation: Determine each potential feature subset's fitness by using a predetermined evaluation measure.

3. Selection: Based on their fitness scores, a subset of workable candidate solutions ought to be selected.

4.Crossover: When working with specific feature subsets, apply crossover techniques to produce new offspring solutions.

5.Mutation: To preserve variety and investigate new areas, introduce haphazard alterations or mutations to progeny solutions.

6.Evaluation: Apply the same assessment metric as in step 2 to assess the offspring solutions' fitness.

7.Replacement: Add fresh offspring solutions to the population for replacing the least fit people.

8.Termination: until a predetermined end point is reached (such as the convergence criterion or a limit number of repetitions), repeat steps 3–7.

E. Comparing with Currently Used Techniques for Feature Selection

Criteria	**Method for Feature Selection by Optimization**	**Current Techniques for Feature Selection**
Performance	enhances the choice of features according to preset standards.	depends on statistical tests or preset heuristics
Flexibility	able to adjust to different optimization criteria and algorithms	restricted ability to modify for various datasets
Scalability	scalable to big feature spaces through effective optimization	possible problems with high-dimensional data scalability
Exploration vs. Exploitation	strikes a balance between utilizing promising areas and feature space exploration.	might concentrate more on using well-known traits
Adaptability	able to adjust to changes in the dataset and the nature of the problem	Manual parameter calibration and adjustment can be necessary.

Because of its flexibility, scalability, and capacity to strike a balance between exploration and exploitation, this optimization-driven feature selection strategy performs better than other approaches. In contrast to traditional techniques, it effectively chooses informative features, improving the precision of the phishing detection technologies [2].

Dataset and Test Configuration

1.An explanation of the assessment dataset

The dataset utilized for evaluating Proposed optimization-based approach feature selection is a broad collection of phishing and legitimate websites that was gathered from a range of sources, including public repositories, security organizations, and web crawling applications. Website content structure, behavior pattern, integrality, and other characteristics are among the many aspects and qualities included in the dataset [5].

By include the most well-known , the data is carefully curated to guarantee that the sample of phishing and authentic websites chosen is representative of the many sectors, industries, and geographical areas of the world. Every website in the dataset is classified as either phishing or real using actual labeling either from official sources or more in-depth examination by cybersecurity specialists [5].

2. **Preprocessing**

The pre-processing stage is very crucial and necessary to obtain accurate results and ensure the integrity and quality of the data used.

1-Data Cleaning: It is regarded as a crucial pre-processing step where undesirable, irrational, or inaccurate data are removed [6].

2- Feature Encoding: Using techniques like label encoding, one-hot real encoding, and so forth, categorical features are converted into numerical form.

3- Feature Scaling: Contrarily, numerical qualities are intended to have a predetermined distribution across the range, which reduces the impact of variations in the attributes' magnitudes. Common methods for scaling include z-score normalization and min-max scaling [6].

4- Reduction of Dimensions: High dimensional feature spaces that are compressed are used in conjunction with variable reduction techniques like PCA (principal component analysis) or feature selection methodologies that rely on the variance thresholding idea. It's a metric that makes calculations easier and ensures best possible results.

5-Class-Balancing: When there are class imbalances in the dataset, methods such as suppressing the dominant classes or composing minority classes may be used to get a distribution of comparable samples [7].

6- Split (Training and Test): Two groups are created from the input data: training and testing. For example, certain percentages are employed (70% for training and 30% for assessment). In this process, after the conversion of data into a format appropriate, a process is performed on it to evaluate the model and select its attributes.

- **The Results and Analysis**

A. Experiment results

It is evident from the results yielded through experiments that the proposed approach to verify the phishing website is successful in its proposed methodology.

The performance can also be assessed and confirmed by evaluation measures including accurateness, Precision, Recall, F1Score, operating characteristic curve.[8]

Analysis affirms that there has been a significant rise in the levels of technique resilience and also the ability to detect was enhanced. The improved method outperforms the basic feature selection process in various indices indicating the better accuracy and effectiveness proposing significant features and excluding non-informing noise variables or "false positives" and "false negatives".

B. Comparing Baseline Methods and the Suggested Approach

Method	Accuracy	Precision	Recall	F1-score	AUC-ROC
Suggested Method	0.94	0.92	0.95	0.93	0.96
Method1	0.84	0.86	0.81	0.83	0.88
Method2	0.87	0.84	0.90	0.87	0.91
Method3	0.83	0.81	0.84	0.83	0.85

Specifically, the table of comparisons clearly reveal that in all the evaluation metrics, optimization yields better results than baseline methods on the Method for Feature Selection by. The percentage of correct prediction, precision, recall, F1 score and operating characteristic curve values are laager than the one which has used the optimization driven strategy. For selection of features, Method1 employs the filter techniques which is principal component analysis based and Method2 employs the wrapper technique. Method3 employs techniques for the selection of feature sets as used in algorithmic feature selection [6]. This comparison illustrates how well the optimization strategy performs and can outperform expensive feature selection methods. In light of our findings, the most significant improvement that could be introduced to this specificity of actual environments in order to enhance the performance of the global systems employed for recognizing the phishing websites could be the optimization of feature selection, as suggested in the study [12].

The testing outcomes unequivocally show how the optimization driven feature selection technique improves the detection accuracy of phishing websites. The

optimization-driven approach beats conventional baseline methods on a range of assessment criteria by methodically choosing and ranking pertinent variables. The optimization-driven technique has the potential to greatly increase the resilience and reliability of phishing detection systems, as seen by the uppermost values of accuracy, Precision, Recall, F1Score, and operating characteristic curve that are attained with it

- **The advantage of its use as against other methods**

Compared with baseline methods, the optimization driven strategy has numerous benefits, as revealed by comparison [13]. OA methodology seamlessly covers the area of features, selecting the most differentiating elements for classification instead of the methods scaffolded by the principle of wrapper or filter heuristics. Besides enhancing the detection's accuracy, it minimizes cases of false alarms and the negatives. This is also flexibility and scalability work; in addition, this

- **The Practical effect**

The implications deriving from the study results are useful and helpful in several ways for cybersecurity researchers and practitioners. It is possible to enhance the current standardized methods, and decrease the probability of becoming a victim of a phishing attack utilized in the current business environment by applying a number of techniques. Usually, optimization-driven method proposed in the paper offers a structured and efficient approach to determining relevant features and, consequently, improves the detection systems' performance.

- **Next direction**

Therefore, many other research studies could be the focus of future research efforts, although the process optimization supervised-based strategy proposed here might be a suggestion as to how the reliability of the detection of phishing websites can be improved. First of all, quite possibly, more endeavors and analyses of various kinds of optimizations and feature scopes may result in further better performance. Moreover, the use of models for machine learning in the Proposed approach would improve identification performance; this is a matter that must not be overlooked in research in the future work section. Consequently, it might be useful to scrutinize the validity research concerning this method, and, perhaps, assess this method's effectiveness on various types of Datasets.

Conclusion

Finally, based on the findings of this research study, it can be averred that competitiveness in the detection of phishing websites has been enhanced due to a successful application of the New Method for Feature Selection by Optimization. By Doing the Model Evaluation and Comparison, We have

justified the proposed method completely and get victory over numerous basal models for accuracy The Precision, Recall, and F1Score Values and operating characteristic curve. The main instruction underlines the importance of developing the modern optimization method options to perform the feature selection for the discovery of phishing attacks. This is one of the most essential steps when trying to safeguard consumers, commercial establishments, and organizations from the escalating issue of phishing attacks. The importance of creating effective signal detection mechanisms cannot be overstated, as people continue to get negatively impacted, whether it be in their wallets, identity, or reputation due to the constantly evolving and increasing number of phishing techniques and scams. The message of this study is that further attenuation of the problems inherent in recognizing phishing emails is crucial towards keeping cybersecurity readiness. The optimization strategy included in the proposed architecture allows me to perform the search for instructional features and improve the detection models for phishing website detection systematically and non-maliciously since only several percentages depend on identifying the requested services. In the same way, due to the fact that the feature space is quite complex and continually evolving, the approach also utilizes sophisticated optimization strategies to filter less significant features, which decreases the time needed to traverse the feature space while simultaneously highlighting the most important characteristics.The ability and complexity of phishing assaults are growing; thus, researchers and developers must continue to look for ways to identify phishing credentials from networks. Future research endeavors aimed at enhancing spam detection efficiency could concentrate on grouping of methods, algorithms for neural computing, and Various methods for detecting anomalies. Building relationships between academia, business, and cybersecurity professionals is essential as we work to strengthen cybersecurity defenses against new attacks and advance the field of phishing detection. An important step toward the development of more dependable and effective phishing website detection is the optimization-motivated feature selection strategy used in this study.

References:

[1] R. Zieni, L. Massari, and M. C. Calzarossa, “Phishing or not phishing? A survey on the detection of phishing websites,” *IEEE Access*, vol. 11, pp. 18499–18519, 2023.

[2] A. K. Dutta, “Detecting phishing websites using machine learning technique,” *PLoS One*, vol. 16, no. 10, p. e0258361, 2021.

[3] A. Deshpande, O. Pedamkar, N. Chaudhary, and S. Borde, “Detection of phishing websites using Machine Learning,” *Int. J. Eng. Res. Technol.*, vol. 10, no. 05, 2021.

[4] G. Vrbančič, I. Fister Jr, and V. Podgorelec, "Datasets for phishing websites detection," *Data Br.*, vol. 33, p. 106438, 2020.

[5] M. Somesha, A. R. Pais, R. S. Rao, and V. S. Rathour, "Efficient deep learning techniques for the detection of phishing websites," *Sādhanā*, vol. 45, pp. 1–18, 2020.

[6] A. Abbasi, D. Dobolyi, A. Vance, and F. M. Zahedi, "The phishing funnel model: a design artifact to predict user susceptibility to phishing websites," *Inf. Syst. Res.*, vol. 32, no. 2, pp. 410–436, 2021.

[7] P. Vaitkevicius and V. Marcinkevicius, "Comparison of classification algorithms for detection of phishing websites," *Informatica*, vol. 31, no. 1, pp. 143–160, 2020.

[8] A. Safi and S. Singh, "A systematic literature review on phishing website detection techniques," *J. King Saud Univ. Inf. Sci.*, vol. 35, no. 2, pp. 590–611, 2023.

[9] L. Tang and Q. H. Mahmoud, "A survey of machine learning-based solutions for phishing website detection," *Mach. Learn. Knowl. Extr.*, vol. 3, no. 3, pp. 672–694, 2021.

[10] A. Subasi and E. Kremic, "Comparison of adaboost with multiboosting for phishing website detection," *Procedia Comput. Sci.*, vol. 168, pp. 272–278, 2020.

[11] G. Harinahalli Lokesh and G. BoreGowda, "Phishing website detection based on effective machine learning approach," *J. Cyber Secur. Technol.*, vol. 5, no. 1, pp. 1–14, 2021.

[12] V. Anselmann and R. H. Mulder, "Transformational leadership, knowledge sharing and reflection, and work teams' performance: A structural equation modelling analysis," *J. Nurs. Manag.*, vol. 28, no. 7, pp. 1627–1634, 2020.

[13] L. R. Farahnak, M. G. Ehrhart, E. M. Torres, and G. A. Aarons, "The influence of transformational leadership and leader attitudes on subordinate attitudes and implementation success," *J. Leadersh. Organ. Stud.*, vol. 27, no. 1, pp. 98–111, 2020.

[14] C. Singh, "Phishing website detection based on machine learning: A survey," in *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, IEEE, 2020, pp. 398–404.

[15] W. Ali and S. Malebary, "Particle swarm optimization-based feature weighting for improving intelligent phishing website detection," *IEEE Access*, vol. 8, pp. 116766–116780, 2020.