International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Improved Detection of Phishing Websites using Machine Learning

Sumo Sami M Aldaham [1], Osama Ouda[1], A.A. Abd El-Aziz[2,3]

Submitted: 07/02/2024 **Revised**: 15/03/2024 **Accepted**: 21/03/2024

Abstract: Phishing attacks pose a significant threat in the cyber landscape, compromising the security of millions by exploiting trust in seemingly legitimate websites. These attacks deceive users into divulging sensitive information, posing substantial challenges to both individual and organizational security. The sophistication of phishing tactics, such as spear phishing and whaling, necessitates advanced detection methods beyond traditional rule-based systems. This paper addresses this issue by employing machine learning techniques to accurately identify and classify phishing websites. We deployed various machine learning models, including Decision Tree, Support Vector Machine (SVM), Artificial Neural Network (ANN), and Random Forest (RF), rigorously testing and evaluating their efficacy in detecting phishing attacks. The dataset used in this paper was sourced from PhishTank.org, providing a real-world context for our models. Preprocessing steps included artifact removal, normalization, and handling data inconsistencies to enhance model performance. These steps ensure that the models processed the most relevant and accurate information, improving their ability to differentiate between legitimate and malicious websites. The results of this study are promising, as the decision tree model showed the highest accuracy at 96.7%, followed by the random forest model at 95.75%. These results confirm the ability of these models to effectively detect phishing sites. The ANN model, despite the challenges of overfitting, highlighted the potential of deep learning in this area, suggesting that with further fine-tuning and regularization, it could provide more powerful detection capabilities. The SVM model's low accuracy of 83.8% was not sufficient. Instead, it provided important insights into what types of phishing strategies require different or more precise detection methods. This finding is critical for developing more targeted models in the future paper.

Keywords: *Website Phishing Detection; Machine Learning; Cybersecurity; Support Vector Machine; Decision Tree; Artificial Neural Networks*

1. Introduction

Phishing attacks have become a pervasive threat in the digital world, compromising the security of millions of users by exploiting their trust in seemingly legitimate websites. These malicious activities deceive users into divulging sensitive information, such as login credentials, credit card numbers, and other personal data, which can lead to significant financial and reputational damage for both individuals and organizations. The increasing sophistication of phishing tactics, including techniques like spear phishing and whaling, has made it essential to develop more advanced detection methods beyond traditional rule-based systems.

Phishing attacks have evolved significantly over the years, becoming more complex and harder to detect. Traditional methods of phishing detection, which often rely on blacklists and heuristic rules, are no longer sufficient to combat these sophisticated threats. Attackers continuously adapt their strategies to bypass these defenses, making it increasingly difficult to protect users effectively. The dynamic nature of phishing schemes, combined with their ability to mimic legitimate user interfaces and communication, poses a substantial challenge for traditional cybersecurity measures.

Spear phishing, for instance, involves highly targeted attacks where the perpetrator tailors their approach to a specific individual or organization, often using personal information to increase the likelihood of success. Whaling, a variant of spear phishing, targets high-profile individuals within an organization, such as executives, by crafting personalized messages that appear to come from trusted sources. These advanced tactics highlight the need for more sophisticated detection mechanisms capable of identifying and mitigating such threats in real-time.

Given the limitations of traditional phishing detection methods, there is a pressing need for innovative solutions that can effectively identify and classify phishing attempts. The primary challenge lies in developing systems that can adapt to the ever-evolving landscape of phishing attacks. This requires leveraging advanced technologies that can learn from past incidents and improve their detection capabilities over time. Machine learning offers a promising approach to address this challenge. By analyzing large datasets of phishing and legitimate websites, machine learning models can identify patterns and features that distinguish malicious sites from safe ones. These models

[1] *Department of Computer Science*
College of Computer and Information Sciences
Jouf University, Sakaka 72388, Saudi Arabia
Email: 441205054@ju.edu.sa, omalsayed@ju.edu.sa
[2] *Department of Information Systems*
College of Computer and Information Sciences
Jouf University, Sakaka 72388, Saudi Arabia
Email: aaeldamarany@ju.edu.sa
[3] *Department of Information Systems and Technology*
Faculty of Graduate studies for Statistical Research, Cairo University, Egypt

can then be trained to detect phishing attempts with high accuracy, even as attackers modify their tactics.

In this paper, we propose a comprehensive approach to phishing detection using machine learning techniques. We employ a variety of machine learning models, including Decision Tree, Support Vector Machine (SVM), Artificial Neural Network (ANN), and Random Forest (RF), to assess their effectiveness in identifying phishing websites. Each model has its strengths and weaknesses, and by evaluating them rigorously, we aim to determine the most effective approach for phishing detection. The dataset used for this paper is primarily sourced from PhishTank.org, a widely recognized repository for phishing URLs. This dataset provides a real-world context for our models, ensuring they are trained and tested against a representative sample of phishing threats. To prepare the dataset for analysis, we implemented several preprocessing steps, including artifact removal, normalization, and handling data inconsistencies. These steps were crucial to refining the input data and enhancing the performance of our machine learning models. Our methodology involves splitting the dataset into training and testing subsets, allowing us to evaluate the models' performance on unseen data. We then apply various metrics, such as accuracy, precision, recall, and F1-score, to measure each model's effectiveness in detecting phishing attempts. By comparing these metrics, we can identify the strengths and limitations of each model and determine the best approach for real-world phishing detection.

This paper is organized to provide a comprehensive understanding of our approach to improving phishing detection using advanced machine learning techniques. The structure is designed to guide the reader through the problem background, methodology, results, and conclusions systematically. The Introduction section introduces the problem of phishing attacks, providing context on their significance and the challenges they pose to cybersecurity. It defines the problem, outlines our proposed solution using machine learning models, and explains the organization of the paper. The Literature Review surveys existing methodologies and approaches to phishing detection, emphasizing the advancements and limitations of current techniques. It provides a critical review of previous paper, setting the stage for our study by highlighting the need for improved detection methods. The Research Methodology details our methodological approach to phishing detection. It covers the data collection process, describing how we sourced our dataset from PhishTank.org. It also explains the preprocessing steps taken to clean and standardize the data, ensuring it is suitable for machine learning analysis. Additionally, it outlines the development and training of various machine learning models, including Decision Tree, Support Vector Machine (SVM), Artificial Neural Network (ANN), and Random Forest (RF). Finally, this section describes the evaluation metrics used to assess the performance of these models. The Results and Discussion section presents the findings of our study, comparing the performance of different machine learning models. It discusses the implications of these results, highlighting the most effective models for phishing detection and identifying areas for improvement. The Conclusion summarizes the key insights gained from our paper, emphasizing the potential of machine learning in enhancing phishing detection. It also outlines directions for future paper, suggesting ways to further improve the robustness and accuracy of phishing detection systems. This structured approach ensures that the reader can follow our paper journey from identifying the problem to proposing a solution, evaluating its effectiveness, and considering future improvements.

2. BACKGROUND

Phishing attacks, characterized by deceptive practices where attackers impersonate legitimate entities to steal sensitive data, pose serious threats across various digital platforms. These platforms range from emails and social media to malicious websites designed to capture personal and financial information. The ramifications of phishing attacks are extensive, affecting not just individual victims but also large organizations by compromising data integrity, financial security, and overall reputation.

These cyber-threats continue to evolve in complexity, often outpacing the capabilities of traditional cybersecurity measures. Phishing schemes have become increasingly sophisticated, using advanced tactics like spear phishing, whaling, and pharming that require more than basic filters and rule-based detection systems. The dynamic nature of phishing attacks, combined with their ability to adapt and mimic legitimate user interfaces and communication, makes them particularly challenging to detect and mitigate.

2.1. Research Questions

- RQ1: How can machine learning algorithms be optimized to accurately differentiate between phishing and legitimate websites based on URL characteristics and content analysis?
- RQ2: What role do evolving phishing techniques play in the development of machine learning models for phishing website detection?
- RQ3: Can machine learning models be trained to predict the emergence of new phishing websites before they become active threats?
- RQ4: How effective are the selected machine learning techniques in detecting complex phishing websites compared to other traditional cybersecurity methods?
- RQ5: What challenges do machine learning models face in real-time phishing website detection, and how

can these challenges be addressed to improve detection rates?

On the one hand, Paper Question 1 (RQ1) probes into the optimization of machine learning algorithms to discern between phishing and legitimate websites effectively. This exploration is critical for pinpointing which algorithms when applied to URL characteristics and content analysis, yield the highest accuracy in phishing detection. It aims to unearth the intricate balance between algorithm complexity and detection precision, ensuring that the chosen models are both efficient and scalable for practical cybersecurity applications. On the other hand, Paper Question 2 (RQ2) delves into the impact of evolving phishing techniques on the development of these machine-learning models. It emphasizes the necessity for adaptive models that can not only recognize current phishing patterns but also learn from emerging threats. This question is pivotal in constructing a dynamic defense mechanism that stays ahead of cybercriminals' continually evolving tactics.

Meanwhile, Paper Question 3 (RQ3) expands the horizon by questioning the predictive power of machine learning models against the inception of new phishing sites. It investigates the potential for these models to act not just reactively but proactively, identifying likely phishing threats before they materialize into active attacks. This forward-looking approach could revolutionize phishing defense strategies, shifting from a stance of response to one of anticipation.

Paper Question 4 (RQ4) explores the effectiveness of selected machine learning techniques in detecting complex phishing websites and compares these with traditional cybersecurity methods. This inquiry is pivotal in assessing how advanced ML algorithms measure up against conventional security measures in identifying sophisticated phishing threats. The goal is to ascertain if the detailed analysis facilitated by these ML models leads to a significant improvement in detection rates in real-world scenarios, offering a more potent defense against the evolving landscape of phishing attacks.

Lastly, Paper Question 5 (RQ5) confronts the practical challenges machine learning models face in real-time phishing detection. It aims to unravel the barriers to implementing these models in live environments, where phishing websites must be identified and neutralized swiftly to prevent harm. Addressing these challenges is vital for enhancing the real-time operational efficiency of phishing detection systems, ensuring they can provide immediate protection against phishing threats as they arise.

Collectively, these paper questions forge a comprehensive inquiry into leveraging machine learning for phishing website detection. They address the spectrum from theoretical optimization of algorithms and features to practical challenges of real-world application, laying the groundwork for significant advancements in cybersecurity defenses against phishing.

2.2. Paper Contributions

- Develop a machine learning-based framework that can efficiently and accurately detect phishing websites.
- Evaluate and compare the effectiveness of various machine learning algorithms in identifying phishing activities.
- Enhance the adaptability and responsiveness of phishing detection systems to cope with the continually evolving tactics used by cybercriminals.
- Integrate the proposed machine learning detection system into existing cybersecurity frameworks to improve real-time detection capabilities and reduce the incidence of phishing attacks.

3. LITERATURE REVIEW

The continuous evolution of cyber threats, especially phishing attacks, underscores the urgent need for effective detection methods. Phishing attacks, deceptive in nature, aim to trick users into divulging sensitive information by masquerading as legitimate entities. The surge in such threats has propelled the adoption of machine learning (ML) and deep learning as forefront technologies in identifying and neutralizing these risks. The primary purpose of these technologies is to augment the accuracy and speed of phishing detection, thereby ensuring a more secure digital environment for users [1]. A cornerstone in this paper is the utilization of consistent datasets like PhishTank, renowned for its comprehensive compilation of verified phishing URLs alongside legitimate websites. This dataset enables researchers to benchmark and compare the efficacy of various machine learning models accurately. For instance, A. K. Dutta (2021) leveraged this dataset to explore the potential of Random Forest and Support Vector Machine (SVM) classifiers in phishing detection, achieving a remarkable accuracy of 95.7% with the Random Forest model. This result underscores the model's adeptness at discerning between phishing and legitimate content, benefiting from the ensemble method's inherent capability to minimize variance and bias [1]. Jain A.K. & Gupta B.B. (2018) also tapped into the rich resource of the UCI Machine Learning Repository's Phishing Websites dataset to develop "PHISH-SAFE." Utilizing a Decision Tree classifier, they managed to detect phishing URLs with an accuracy of 92.3%. The simplicity of Decision Trees, combined with their interpretability, makes them invaluable for rapid assessments and decisions in phishing detection scenarios [2]. Exploring further, Purbay M. & Kumar D. (2021)

evaluated the efficacy of SVM against other supervised algorithms like Naïve Bayes and K-Nearest Neighbors (KNN). Their study highlighted SVM's superiority, achieving an accuracy of 93.8%. The model's success stems from its capacity to effectively manage the high-dimensional spaces characteristic of phishing data, thereby enhancing detection [3].In a different vein, Gandotra E. & Gupta D. (2021) employed Gradient Boosting on the same dataset, attaining an accuracy of 94.5%. This study illuminated the power of boosting techniques in phishing detection by iteratively refining models to correct previous errors, thereby progressively improving accuracy [4]. Hung Le et al. (2017) took a deep learning approach with Convolutional Neural Networks (CNN) in their "URLNet" system. Applied to a dataset combining PhishTank and Alexa's top websites, URLNet achieved an F1-score of 97.2%, highlighting CNNs' ability to autonomously extract complex features from URLs. This capability is critical for learning the intricate patterns embedded in URLs, making CNN a powerful tool in phishing detection. However, its reliance on significant computational resources and a robust training regime is a consideration for its deployment [5].

Integrating lexical features and block-listed domains into phishing detection, Hong J. et al. aimed to refine the detection process, achieving an accuracy of 91%. This integrated approach leveraged machine learning models to enhance traditional block-listing methods, offering a dynamic response to evolving phishing threats. However, this method's effectiveness is less pronounced against completely new or previously unseen phishing sites [6].J. Kumar et al. (2020) reaffirmed the effectiveness of the Random Forest classifier, achieving 96% accuracy on the UCI dataset. The model's ability to manage large and diverse datasets without significant overfitting is a testament to its utility in phishing detection. It underscores the importance of feature diversity and the classifier's capacity to manage various indicators of phishing [7]. Aljofey A. et al. (2020) explored the use of a character-level convolutional neural network model, reaching an impressive F1 score of 98% on a mix of PhishTank and DMOZ datasets. This approach, particularly potent at the character level, was effective in identifying subtle anomalies in URLs. This achievement highlights the potential of neural networks to detect sophisticated phishing attempts that might elude simpler detection systems [10].AlEroud A. & Karabatis G. (2020) investigated the application of generative adversarial networks for refining phishing detection, reaching an accuracy of 94%. This novel approach proved that generative models could simulate and learn from adversarial attacks, thus enhancing the resilience of phishing detection systems [11]. The sample sizes and diversity in these studies are pivotal for generalizing the findings. Studies using larger and more varied samples enable the detection of nuanced phishing tactics. This is clear in the works of researchers like Aljofey et al., who, by using mixed datasets, could discern complex phishing behaviors, a crucial step in developing effective countermeasures [10]. The results across these studies consistently highlight that machine learning and deep learning significantly enhance phishing detection. The adaptability of these models to new threats, coupled with their ability to process vast amounts of data, positions them as essential tools in the ongoing fight against cybercrime. However, there is room for further exploration and integration of these methodologies to keep pace with the rapidly evolving landscape of phishing and other cyber threats.

4. RESEARCH METHODOLOGY

The methodology adopted for this paper is designed to explore the efficacy of machine learning (ML) algorithms in detecting phishing websites, which is essential for the advancement of cybersecurity measures. This section elaborates on the systematic approaches used in data collection, feature selection, and engineering, model development, and the evaluation frameworks implemented to measure the performance and reliability of the proposed models.

4.1. Data Collection

The dataset used in this study, which is essential for detecting phishing sites, was meticulously compiled from two main sources. Initially, much of the data was downloaded from PhishTank.org, a reputable source known for its comprehensive and regularly updated repository of verified phishing URLs. Additionally, to enrich the dataset and ensure a broad representation of phishing characteristics, we combined data from the final dataset used in the study by A. K. Dutta [1], which includes both phishing URLs and legitimate website URLs.

The dataset includes a total of 10,000 instances, evenly divided with 5,000 instances classified as phishing and 5,000 instances classified as non-phishing.

This balanced approach allows for a fair comparison between models and helps to prevent any bias that might arise from uneven class distribution. Each instance in the dataset is characterized by features that are critical for distinguishing phishing sites from legitimate ones. Table 1 shows features like the URL structure, domain attributes, and the use of secure protocols…etc

Table 1. Features Selection

Seq	Feature	Meaning
1	Domain	Main part of the URL, Helps find known malicious or safe domains
2	Have_IP	Presence of an IP address in the URL, IP in URL can indicate a phishing attempt
3	Have_At	Presence of '@' symbol, used to mislead users about the link's destination
5	URL_Length	Length of the URL Longer URLs are often associated with phishing
6	URL_Depth	Number of '/' in the URL, Deeper pages can indicate phishing
7	Redirection	Presence of redirection mechanisms, used to redirect users to malicious sites
8	https_Domain	If the domain starts with 'https', Misused by phishers to create a false sense of security
9	TinyURL	Usage of URL shortening services, Obscures the actual destination
10	Prefix/Suffix	Presence of '-' in the domain, Uncommon in legitimate domains
11	DNS_Record	Existence of a DNS record for the domain, most legitimate sites have DNS records
12	Web_Traffic	Level of web traffic to the URL, Legitimate sites usually have higher traffic
13	Domain_Age	Age of the domain, newer domains more likely used in phishing
14	Domain_End	How close the domain is to its expiration date; Phishers often use domains that are about to expire
15	iFrame	Usage of iframes on the website, could be used to embed malicious content
16	Mouse_Over	Presence of script functions that execute on mouse hover, can be used maliciously
18	Right_Click	If the website disables right-click functionality, Prevents users from inspecting web elements
19	Web_Forwards	Presence of automatic forwards, another method to lead users to phishing sites

4.1.1. Division of the Dataset

To train and evaluate the machine learning models effectively, the dataset was partitioned into two subsets:

- Training Set: 80% of the dataset, or 8,000 instances, was allocated for training the models. This subset includes 4,000 phishing and 4,000 non-phishing instances. The training set is crucial for the models to learn the distinguishing features of phishing and legitimate websites.
- Test Set: The remaining 20%, consisting of 2,000 instances (1,000 phishing and 1,000 non-phishing), formed the test set. This division ensures that the models are evaluated on data they have not seen during training, providing a measure of their generalization capability and accuracy in real-world scenarios.
- To ensure our machine learning models are both trained and tested under realistic conditions, we divided the dataset into two segments:
- Training Set: Including 80% of the total instances (8,844 instances), this segment is used to train the models. It includes a mix of phishing and legitimate labels, providing the models with ample examples to learn from and adapt to various

phishing tactics and legitimate behaviors.

- Test Set: The remaining 20% of the data (2,211 instances) forms the test set. This segment is crucial for evaluating the trained models against unseen data, assessing their generalization capabilities, and ensuring they keep high accuracy and reliability when deployed in real-world scenarios.

This structured approach to data collection and division is foundational to enhancing the accuracy and reliability of our phishing detection system. By training our models on a dataset that closely mirrors the complex dynamics of real-world web interactions, we ensure that our system is prepared to effectively combat the ever-evolving landscape of cyber threats.

4.2. Data Preprocessing

Since the dataset encompasses a variety of URL structures, domain information, and textual content, each with its peculiarities, the data preprocessing step in this paper was crucial. To address such variances, a normalization method was employed as described in Eq. (1), transforming the numerical features to a common scale without distorting differences in the ranges of values. This was achieved by standardizing each feature value using the following formula:

$$X_{std} = \frac{X - \mu}{\sigma} \quad (1)$$

Here, X_{std} represents the standardized value, X is the original value, μ is the mean of the feature values, and σ is the standard deviation of those values. This transformation ensures that each feature contributes equally to the model, thereby improving the learning efficiency and stability of the machine learning algorithms.

Furthermore, to help the analysis and model training, categorical attributes were converted into a numerical format through label encoding and, where necessary, one-hot encoding. This ensured that models could interpret the data correctly without being misled by non-numerical values.

To address variations in categorical data and enhance model interpretability, the categorical features were processed using the approach outlined in Eq. (2). The value transformation for each categorical feature was performed by mapping each unique category to a distinct integer value, normalizing the categorical diversity across the dataset.

$$Category_{encoded} = index(category) \quad (2)$$

Each preprocessing step, from feature standardization to categorical encoding, was designed to improve the dataset's structure, facilitating more accurate and efficient phishing site detection by the machine learning models.

4.3. Model Development and Evaluation

To address the paper objectives, multiple ML models were developed and rigorously evaluated. Each model was chosen based on its proven track record in classification tasks, particularly in the domain of cybersecurity.

4.3.1. Machine Learning Models

- Decision Trees are fundamental to the field of machine learning, known for their straightforward and transparent approach to classification and regression tasks. These models operate by creating a tree-like structure where each node represents a feature of the dataset, and branches denote the decision rules leading to different outcomes. The simplicity of Decision Trees lies in their ability to break down complex decision-making processes into a series of simpler, binary choices, making the model's decisions easy to interpret and explain. This characteristic is particularly advantageous in phishing detection, as it allows security analysts to understand and trace the reasoning behind each classification. Moreover, Decision Trees can manage both numerical and categorical data, making them versatile for various types of input features commonly encountered in phishing datasets.
- Support Vector Machines (SVM): Support Vector Machines are powerful, supervised learning models used for classification and regression tasks. SVMs are particularly noted for their ability to create optimal hyperplanes in a multidimensional space that distinctly classifies the data points. This capability is crucial in phishing detection, where the distinction between phishing and legitimate websites often lies in subtle and high-dimensional differences in features. SVMs are robust against overfitting, especially in high-dimensional spaces, due to their regularization parameter, which helps maintain the generalizability of the model. Their effectiveness in dealing with non-linear boundaries, thanks to kernel tricks, allows them to adapt to the complex and evolving nature of phishing attacks.
- Neural Networks: Neural Networks represent a more advanced tier of machine learning models, inspired by the neural structure of the human brain. Comprising layers of interconnected nodes or "neurons," these networks can model highly complex, non-linear relationships in data. The depth and flexibility of Neural Networks make them exceptionally suited for phishing detection, where attackers constantly innovate and vary their techniques. The layered architecture allows Neural Networks to learn from a vast amount of data and recognize intricate patterns that simpler models might miss. This capability is

pivotal in identifying sophisticated phishing schemes that employ advanced cloaking, scripting, and social engineering tactics.

- Random Forest Classifier: The Random Forest Classifier extends the concept of Decision Trees into a more powerful ensemble method that combines multiple trees to improve the predictive performance and reduce the risk of overfitting. Each tree in a Random Forest works on a random subset of features and data points, leading to a diverse set of classifiers whose results are aggregated to produce a final decision. This diversity makes Random Forests particularly effective in phishing detection, as they can capture a wide array of indicators of malicious behavior without being overly sensitive to noise and outliers in the data. The ensemble approach also means that Random Forests are less likely to be swayed by deceptive techniques used by phishing attacks, providing a robust defense against a variety of phishing tactics.

4.3.2. Key Metrics for Assessing Machine Learning Models

The models were evaluated using a suite of metrics to assess their predictive accuracy and generalizability:

Accuracy: This essential metric gauges the model's overall correctness across all classes. It is the ratio of correctly predicted instances to the entire set of instances within the dataset, formalized as shown in Eq. (3):

$$Accuracy = \frac{Number\ of\ Correct\ Predictions}{Total\ Number\ of\ PredictionsNumber} \quad (3)$$

Precision: This metric elucidates the model's capability in accurately predicting positive (phishing) instances. It captures the proportion of true positives among all positive predictions, as delineated in Eq. (4):

$$Precision = \frac{True\ Positives}{True\ Positives + False\ Positives} \quad (4)$$

Recall: Known as the sensitivity or true positive rate, recall indicates the model's proficiency in identifying all pertinent phishing instances. This is computed as the ratio of true positives to the sum of true positives and false negatives, detailed in Eq. (5):

$$Recall = \frac{True\ Positives}{True\ Positives + False\ Negatives} \quad (5)$$

F1-score: Serving as the harmonic mean of precision and recall, the F1-score offers a balanced metric to evaluate the equilibrium between the model's precision and recall capabilities. This is particularly vital in datasets skewed towards either phishing or legitimate instances. The F1-score is represented in Eq. (6):

$$F1\text{-}score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (6)$$

ROC Curves: The Receiver Operating Characteristic (ROC) curves graphically portray the diagnostic ability of binary classifiers, a cornerstone in phishing detection to balance the trade-offs between true positive rates and false positive rates. The Area Under the Curve (AUC) metric provides a measure of the model's discernment between positive and negative classes, as depicted in Eq. (7):

$$AUC = \int_0^1 TPR(t)dt \quad (7)$$

The comprehensive application of these methodologies aims not only to validate the effectiveness of the ML models in distinguishing between phishing and legitimate websites but also to explore their potential integration into broader cybersecurity frameworks, offering advancements in preemptive cyber defense mechanisms.

5. RESULTS

In this study, we aimed to evaluate the effectiveness of various machine learning models in detecting phishing websites using a comprehensive dataset derived from verified sources. The dataset was preprocessed using label encoding to transform categorical features into a format suitable for model input. This preprocessing step was crucial for facilitating the application of machine learning algorithms on the data.

5.1. Analysis Performance of Models

5.1.1. Visualizing the data:

Before applying machine learning techniques, we conducted an initial analysis to understand the distribution of the various features within our dataset. Each feature's histogram was generated to visualize its distinct patterns and the presence of potential outliers. These visualizations, shown in Fig. 1, demonstrate significant differences in the distributions and ranges of features such as URL length, HTTPS domain presence, and the use of special symbols in URLs.

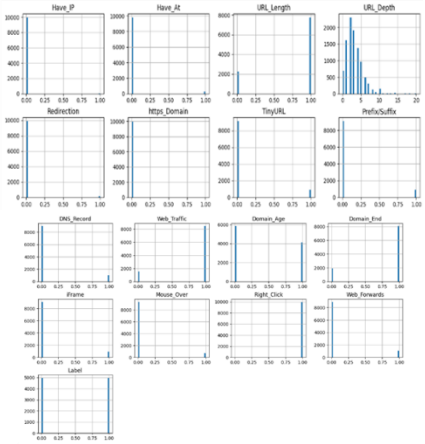

Fig. 1 Visualizing the data

5.1.2. Decision Tree Model:

The Decision Tree model employs a tree-like structure to

make decisions and classify data. By breaking down a dataset into smaller subsets while developing an associated decision tree incrementally, this model handles both linear and non-linear data effectively. One of its main strengths is its interpretability; the model decisions can be easily understood and visualized, making it user-friendly for the explanation and analysis of complex decisions. Additionally, Decision Trees can manage non-linear relationships well, which broadens their applicability across varied datasets. Table 3 provides a summary of the performance of the Decision Tree model. As shown in Fig. 2, the Decision Tree model demonstrates a perfect training accuracy of 100%, indicating a strong fit to the training data. However, the validation accuracy is slightly lower at 96.7%, which suggests minor overfitting. The training loss is nearly zero, while the validation loss stands at 1.14.

Table 2. a summary of the performance of the Decision Tree model

Classification	Value
Training Accuracy	100%
Validation Accuracy	96.7%
Training Loss	~0 (log loss)
Validation Loss	1.14 (log loss)

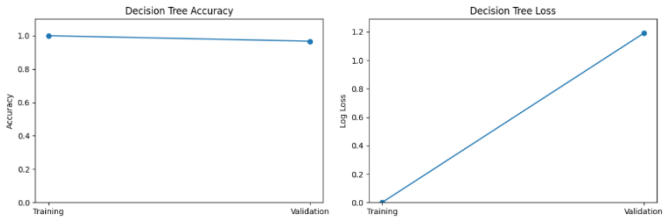

Fig. 2 Accuracy and loss graphs for the Decision Tree model.

5.1.3. Support Vector Machine (SVM):

The Support Vector Machine (SVM) model is designed to identify the optimal hyperplane that maximizes the margin between different classes in a dataset. SVMs are particularly effective in high-dimensional spaces and are versatile using kernel functions, which allow them to adapt to linear and non-linear data. The kernel trick transforms data into a higher dimension where a separating hyperplane can be more easily found, making SVMs powerful tools for complex datasets with intricate patterns. Table 4 provides details of the SVM model's performance. Fig. 3 illustrates the performance of the SVM model. The training accuracy is 84.85%, and the validation accuracy is 83.8%. The closeness of these two values indicates that the model generalizes well without significant overfitting or underfitting. The training and validation losses are 0.348 and 0.369.

Table 3. a summary of the performance of the Support Vector Machine (SVM) model

Classification	Value
Training Accuracy	84.85%
Validation Accuracy	83.8%
Training Loss	0.348 (log loss)
Validation Loss	0.369 (log loss)

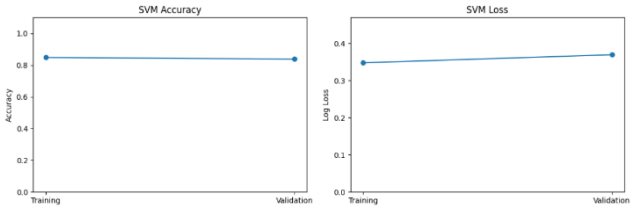

Fig. 3 Accuracy and loss graphs for the SVM model.

5.1.4. Artificial Neural Network (ANN):

Artificial Neural Networks (ANNs) are foundational components of deep learning systems, mimicking the behavior of the human brain to process complex data patterns. Through layers of neurons and the process of backpropagation, ANNs adjust weights based on error rates from previous iterations to improve their predictive capabilities. This iterative adjustment enables ANNs to learn intricate and high-dimensional patterns in large datasets. The results for the ANN model are summarized in Table 5. As shown in Fig. 4, the ANN model achieves a training accuracy of 88.95% and a validation accuracy of 86.85%. These figures suggest that the model maintains consistency across datasets but shows signs of slight overfitting, as evidenced by a lower validation accuracy. The training loss is 0.257, with a validation loss of 0.305, supporting this observation of overfitting.

Table 4. summarized results for the ANN model

Classification	Value
Training Accuracy	88.95%
Validation Accuracy	86.85%
Training Loss	0.257 (log loss)
Validation Loss	0.305 (log loss)

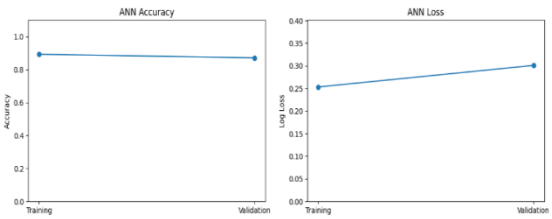

Fig. 4 Accuracy and Loss for the ANN Model.

5.1.5. . Random Forest Classifier:

The Random Forest Classifier enhances the Decision Tree approach by integrating multiple trees to form an ensemble, which significantly improves the model's accuracy and robustness. By averaging the results of individual trees, Random Forest reduces the risk of overfitting that single Decision Trees often face. This ensemble method is effective in handling diverse types of data and complex patterns, making it a strong choice for both classification and regression tasks. Table 6 details the performance of the Random Forest model. Fig. 5 shows the performance of the Random Forest model. The training accuracy is perfect at 100%, while the validation accuracy is an impressive 95.75%. This high accuracy on unseen data demonstrates the model's strong generalization capabilities. The training loss is minimal at 0.022, and the validation loss is 0.135.

Table 5. summarized results for the Random Forest model

Classification	Value
Training Accuracy	100%
Validation Accuracy	95.75%
Training Loss	0.022 (log loss)
Validation Loss	0.135 (log loss)

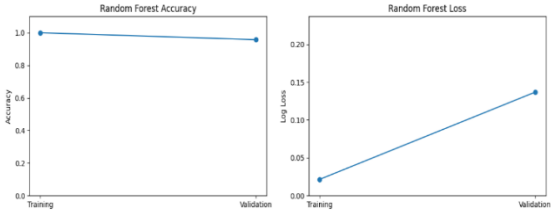

Fig. 5 Accuracy and Loss for the Random Forest Model.

Table 6. summarized results for each model

Model	Training Accuracy	Validation Accuracy	Training Loss	Validation Loss
Decision Tree	100%	96.70%	~0 (log loss)	1.14 (log loss)
SVM	84.85%	83.80%	0.348 (log loss)	0.369 (log loss)
ANN	88.95%	86.85%	0.257 (log loss)	0.305 (log loss)
Random Forest	100%	95.75%	0.022 (log loss)	0.135 (log loss)

The Confusion Matrix is a pivotal tool in machine learning, essential for evaluating the performance of classification models. It delineates the number of correct and incorrect predictions, enabling the identification of the types of errors a model makes. Our study employed four classification models: Decision Tree, Support Vector Machine (SVM), Artificial Neural Network (ANN), and Random Forest Classifier, each assessed using their respective confusion matrices as shown in Fig. 6.

The Decision Tree model exhibited exceptional performance with 992 true negatives (TN) and 942 true positives (TP), while producing only 20 false positives (FP) and 46 false negatives (FN). This indicates a high accuracy, with minimal misclassification.

Conversely, the SVM model showed a significant number of false negatives (296), although it achieved 984 TN and 692 TP, with 28 FP. This suggests that while SVM is effective in identifying negative samples, it struggles with correctly classifying positive instances.

The ANN model performed well, recording 973 TN and 770 TP. However, it had 39 FP and 218 FN, indicating a balanced but slightly less effective performance in comparison to the Decision Tree and Random Forest models.

The Random Forest model demonstrated robustness similar to the Decision Tree, achieving 993 TN and 922 TP, along with 19 FP and 66 FN. This underscores its high accuracy and reliability in classification tasks.

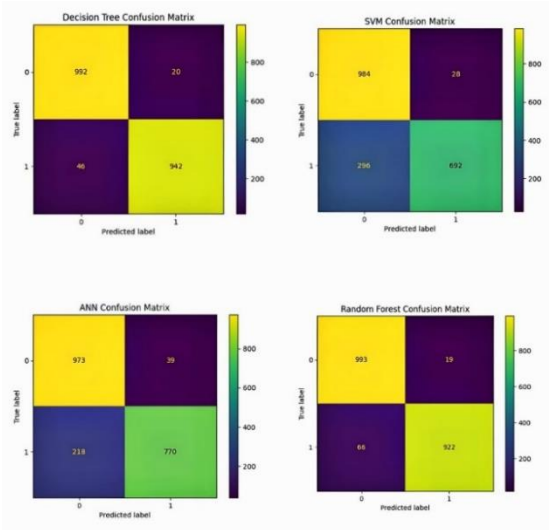

Fig. 6 Confusion Matrices for Various Classification Models

Table 7. results of Performance Metrics for Decision Tree model

Decision Tree Model	Class	Accuracy	Precision	Recall	F1 Score
	Phishing	0.967	0.979	0.953	0.966
	Normal	0.967	0.953	0.979	0.966
	Average	0.967	0.966	0.966	0.966

Table 8. results of Performance Metrics for svm model

SVM Model	Class	Accuracy	Precision	Recall	F1 Score
	Phishing	0.838	0.961	0.700	0.810
	Normal	0.838	0.796	0.929	0.857
	Average	0.838	0.861	0.815	0.834

Table 9. results of Performance Metrics for ANN model

ANN Model	Class	Accuracy	Precision	Recall	F1 Score
	Phishing	0.8715	0.952	0.779	0.857
	Normal	0.8715	0.832	0.952	0.889
	Average	0.8715	0.892	0.8655	0.873

Table 10. results of Performance Metrics for the Random Forest model

RANDOM FOREST MODEL	Class	Accuracy	Precision	Recall	F1 Score
	Phishing	0.9575	0.979	0.933	0.955
	Normal	0.9575	0.940	0.979	0.959
	Average	0.9575	0.959	0.956	0.957

Overall, the Decision Tree and Random Forest models outperformed the others, displaying superior accuracy and lower error rates. The SVM and ANN models, while competent, showed areas for improvement, particularly in reducing false negatives. These insights highlight the efficacy of ensemble methods like Random Forest in achieving optimal classification performance, reinforcing their applicability in tasks requiring high precision and accuracy.

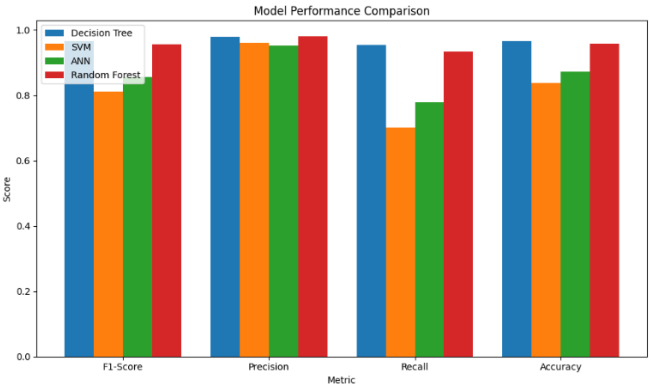

Fig. 7 Model Comparison Bar Chart

5.2. ROC and Precision-Recall Curves Analysis

In this section, we systematically examine the discriminatory capabilities and precision-recall balance of the Decision Tree, SVM, ANN, and Random Forest models in phishing detection. The ROC curves in Fig. 7 collectively display the trade-off between the true positive rate and false positive rate for each model, enabling a comparative analysis of their ability to distinguish between phishing and non-phishing instances across varied thresholds. Similarly, the Precision-Recall curves in Fig. 8 aggregate the models' precision and recall metrics, crucial for assessing performance in our imbalanced dataset context. This integrated approach facilitates a holistic view of the models' strengths and weaknesses, highlighting which models maintain high precision while maximizing recall, and provides a nuanced understanding of their overall effectiveness in differentiating and accurately predicting phishing activities.

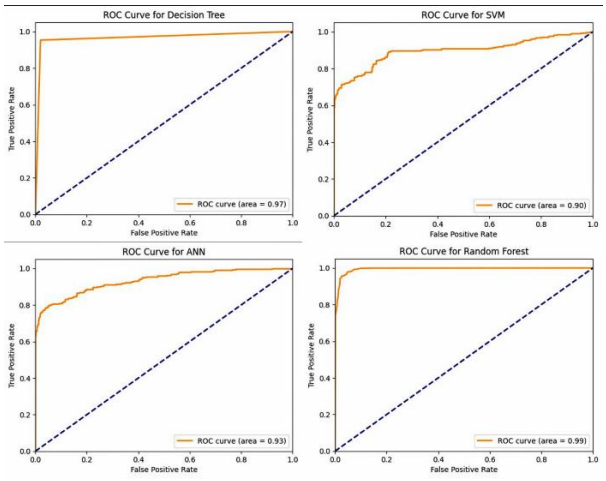

Fig. 8 ROC Curves

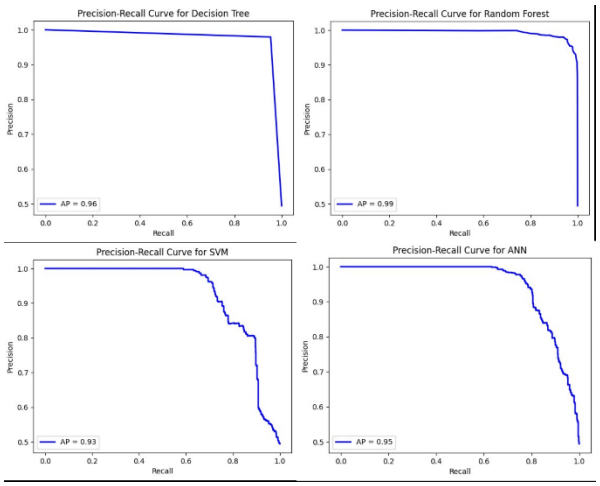

Fig. 9 Precision-Recall Curves

The table presents a comprehensive view of the key metrics used to assess the effectiveness of each model in phishing detection. The Decision Tree model demonstrates exceptional performance across all metrics, with an F1 score of 0.9662, indicating a high balance between precision and recall. This model also shows the highest accuracy at 0.967, making it highly effective in correctly identifying phishing attempts. The SVM model, while showing high precision (0.9611), struggles with recall (0.7004), leading to the lowest F1 score (0.8103) among the models. This suggests that while it is precise in marking positive instances, it misses a significant number of true positives, which is a critical consideration in phishing detection.

The ANN model balances performance with an F1 score of 0.8570 and shows a good precision of 0.9518. However, its recall at 0.7794 and accuracy at 0.8715 indicate some missed phishing instances, suggesting room for improvement in model sensitivity. Lastly, the Random Forest model achieves robust overall metrics, with an F1 score of 0.9559 and the highest precision (0.9798). Its recall of 0.9332 and accuracy of 0.9575 make it highly competitive with the Decision Tree model, offering a strong alternative with consistent performance across various evaluation metrics.

Table 11. Summary of Performance Metrics for Each Model

Model	F1 Score	Precision	Recall	Accuracy
Decision Tree	0.9662	0.9792	0.9534	0.967
SVM	0.8103	0.9611	0.7004	0.838
ANN	0.857	0.9518	0.7794	0.8715
Random Forest	0.9559	0.9798	0.9332	0.9575
Average	0.8974	0.9681	0.8416	0.909

The results of this study were promising, as the decision tree model showed the highest accuracy at 96.7%, followed by the random forest model at 95.75%. These results confirm the ability of these models to effectively detect phishing sites. The ANN model, despite the challenges of overfitting, highlighted the potential of deep learning in this area, suggesting that with further fine-tuning and regularization, it could provide more powerful detection capabilities. The SVM model's low accuracy of 83.8% was not sufficient. Instead, it provided important insights into what types of phishing strategies require different or more precise detection methods.

6. Discussion

The results of this paper are an important step towards improving the detection of phishing sites using advanced machine learning techniques. The analysis of different models' performance highlights the effectiveness and challenges faced by individual models.

The decision tree model showed a high resolution of 96.7% on the verification group, indicating its great ability to distinguish between phishing and legitimate sites. However, the 100% accuracy of training shows the likelihood of over-adaptation, as the model learns the patterns of training data very accurately, which may reduce its ability to generalize new data.

On the other hand, the supporting vector machine (SVM) model provided a reasonable accuracy of 83.8% on the verification kit. This model had the highest accuracy in identifying false positives, which means it is very accurate in identifying non-phishing sites but may fail to detect some phishing sites. This indicates the need to improve the model to include a wider range of sophisticated phishing threats.

The synthetic neural network (ANN) achieved 86.85% accuracy on the verification group, and showed challenges related to over-adaptation. While the results indicate the neural network's ability to learn from complex data, it needs improvement to adjust and modify the model to reduce the gap between training performance and verification.

For the Random Forest model, it showed excellent performance with verification accuracy of 95.75%. This model combines the predictive power of multiple decision trees, reducing the risk of over-adaptation and improving the accuracy of predictions, making it one of the best models used to detect hunting.

These results are consistent with previous papers that has confirmed the effectiveness of various models of machine learning in detecting phishing. For example, in the study A. K. Dutta (2021) the RNN model was used with LSTM and achieved accuracy of 95.7%. Although this model requires substantial accounting resources, it may face difficulties in

handling data in real time. In the study of Jain A.K. & Gupta B.B. (2018) the decision tree model was used and achieved 92.3% accuracy, although this model simply has its complexity and interpretability, its ability to handle complex data is limited. The Purbay M. & Kumar D. (2021) study used the SVM model and achieved 93.8% accuracy, and although this model is effective in managing high-dimensional space, it may face challenges in handling multidimensional data. Gandotra E. & Gupta D. (2021) used Gradient Boosting technology and achieved 94.5% accuracy, a technology based on gradually correcting errors, improving model performance over time. Hung Le et al. (2017), it used CNN (URLNet) and achieved an F1 rate of 97.2%, but this technology requires significant computational resources. Hong J. et al. Machine learning techniques were used with verbal features and achieved 91% accuracy, but were less effective in dealing with new or invisible sites. J. Kumar et al. (2020) Used the random forest model and achieved 96% accuracy, demonstrating the ability to manage large and diverse data without over-adaptation. Study Aljofey A. et al. (2020) used a neural network based on letter analysis and achieved an F1 rate of 98%, as it was effective in detecting nuances in URLs. The AlEroud A. & Karabatis G. (2020) study used generative competitive models and achieved 94% accuracy, demonstrating that generative models can learn from competitive attacks to improve detectability. In contrast, the current study used several models such as decision tree, SVM, ANN and random forest, where the decision tree model achieved resolution of 96.7%, the SVM model achieved resolution of 83.8%, the ANN model achieved resolution of 87.15%, and the random forest model achieved accuracy of 95.75%, As shown in the table 12.

These results demonstrate that each model has its own challenges, such as computational efficiency and over-adaptation in the ANN model, requiring the use of regulatory techniques and reducing the number of parameters to improve generalization capability. In addition, computational efficiency is a major challenge, with models such as neural networks and random forest requiring significant computational resources, which may be an impediment in environments with limited resources. This comparison shows that the results of the current study are consistent with previous studies and emphasizes the importance of using advanced machine learning techniques in detecting phishing, with a focus on improving computational efficiency and adapting new data to achieve better performance in the future.

It should be noted that the nature of phishing data is constantly changing, and the data used may not reflect all current phishing types. Therefore, it is important to use continuously updated datasets and apply continuous learning techniques to ensure that models can adapt to new threats quickly. This study opens doors for future paper in several directions. Combining strengths in multiple models such as integrating decision tree with SVM or ANN can provide a more balanced and effective solution. Lightweight models that maintain high accuracy with computational efficiency can also be developed, using techniques such as Model Pruning or using efficient structures such as MobileNets.

Increasing data diversity by collaborating with security agencies and companies to obtain more comprehensive and up-to-date data sets reflecting the current trolling landscape is essential. Synthetic data generation techniques can be used to train models in varied and difficult scenarios. These results emphasize the potential for machine learning in improving phishing detection, but also highlight the need for continuous improvements and adopt new techniques to keep pace with the evolution of threats. Tackling real-time trolling requires models that can quickly adapt to new threats, making continuous learning or online learning techniques essential in this area.

Table 12. comparative analysis of phishing detection studies

Study	Methodology	Accuracy	Limitations	Dataset
A. K. Dutta (2021)	RNN with LSTM	95.70%	Requires significant computational resources; may struggle with real-time data	PhishTank
Jain A.K. & Gupta B.B. (2018)	Decision Tree	92.30%	Limited complexity, interpretability	UCI Phishing Websites, PhishTank
Purbay M. & Kumar D. (2021)	SVM	93.80%	High-dimensional space management	UCI Phishing Websites, PhishTank
Gandotra E. & Gupta D. (2021)	Gradient Boosting	94.50%	Error correction, iterative refinement	UCI Phishing Websites, PhishTank
Hung Le et al. (2017)	CNN (URLNet)	F1: 97.2%	Significant computati	PhishTank, Alexa Top

			onal resources	
Hong J. et al.	ML with lexical features	91%	Less effective on new/unseen sites	PhishTank
J. Kumar et al. (2020)	Random Forest	96%	Managing large, diverse datasets without overfitting	UCI Phishing Websites, PhishTank
Aljofey A. et al. (2020)	Character-level CNN	F1: 98%	Detecting subtle anomalies in URLs	PhishTank, DMOZ
AlEroud A. & Karabatis G. (2020)	Generative Adversarial Networks	94%	Learning from adversarial attacks to enhance resilience	PhishTank
The proposed model	Decision Tree, SVM, ANN, Random Forest	Decision Tree: 96.7%, SVM:83.8%, ANN:87.15%, Random Forest: 95.75%	Model-specific challenges, computational efficiency, overfitting in ANN	PhishTank

7. Limitations and Future Research

Exploring machine learning techniques for detecting phishing sites, as presented in this study, has led to important insights into the strengths and weaknesses of different models. However, it is necessary to acknowledge the inherent limitations associated with our paper and identify potential directions for future studies. Our paper deployed a suite of machine learning models including Decision Tree, SVM, ANN, and Random Forest to evaluate their effectiveness in detecting phishing sites. While these models showed excellent accuracy, they also showed some limitations that need to be addressed. The main concern is the challenge of overfitting, especially with ANN models. The tendency of artificial neural networks to outgrow training data can reduce their generalizability to new, unseen data sets. This limitation is critical in the context of phishing detection, as attackers are constantly evolving their strategies and models must adapt to new patterns of malicious behavior. Moreover, the computational efficiency of these models poses another challenge. The complexity and depth of models such as ANN and Random Forest can lead to significant computational requirements, especially when processing large data sets or operating in real-time environments. This requirement can hinder the deployment of these models in low-resource environments or applications where fast response time is critical. Another limitation is the heterogeneity of the dataset used in our study. While we use a dataset from PhishTank, the phishing landscape is constantly changing, and the datasets may not be able to capture the full scope of phishing threats. This limitation can affect the models' ability to generalize to all types of phishing attacks, especially those that use new techniques or target specific demographics. Additionally, the study focuses on machine learning models without including deep learning methods such as convolutional neural networks (CNNs) or more advanced recurrent models to explore which techniques may be more effective in detecting phishing. Deep learning models have shown promise in capturing complex patterns in data but were not examined in this study due to their high computational requirements and complexity. In future paper, these limitations should be addressed to increase the robustness and applicability of phishing detection models. One avenue for future work is to explore hybrid models that combine the strengths of different machine-learning techniques. For example, ensemble methods that combine decision trees and meta-models or use a combination of SVM and ANN can compensate for weaknesses such as overfitting or computational inefficiency in individual models. Moreover, developing lightweight models that maintain high accuracy with computational efficiency is essential for real-time phishing detection. Techniques such as model pruning, quantization, or using efficient architectures such as mobile networks can be explored to reduce the computational burden without compromising detection performance. Developing a dataset used in phishing detection paper is another important area for future work. Collaboration with cybersecurity agencies and industry partners will facilitate access to more comprehensive and up-to-date datasets that reflect the current phishing landscape. In addition, the use of synthetic data generation techniques such as generative adversarial networks (GAN) can help create different and challenging scenarios for training and testing phishing detection models. Another promising direction is to incorporate user behavior and contextual data into model training. And prophecy. Understanding user interactions with phishing threats can provide additional insights that improve models' detection capabilities. Techniques such as behavior-based analysis or incorporating contextual features from user environments may lead to a more accurate and personalized phishing detection system. Additionally, meeting the challenge of real-time phishing attacks as new and unknown threats emerge requires models that can learn and adapt in real-time. Incremental learning methods, or online learning strategies, where models constantly update their knowledge as new data arrives, are critical to combating these evolving threats.

8. Conclusion

The proliferation of phishing attacks in the digital age presents a formidable challenge, one that demands innovative and effective solutions. This study's exploration of machine learning models to detect phishing websites has contributed significantly to this ongoing battle, demonstrating the potential of these techniques to enhance cybersecurity measures. Through a detailed examination of various models, including Decision Tree, SVM, ANN, and Random Forest, this paper has highlighted both the strengths and weaknesses inherent in each approach, providing a comprehensive understanding of their capabilities in the context of phishing detection. The Decision Tree model emerged as a standout performer in this study, achieving an accuracy rate of 96.7%, indicative of its robustness and reliability in identifying phishing threats. This model's simplicity and interpretability make it an invaluable tool in the cybersecurity arsenal, especially for rapid assessments and modifications in response to evolving threats. The Random Forest model also showed impressive results, with a 95.75% accuracy rate, underscoring the efficacy of ensemble methods in enhancing detection capabilities by leveraging the strengths of multiple decision trees. While the ANN model demonstrated considerable promise with its deep learning capabilities, it also faced challenges related to overfitting. This limitation underscores the need for careful model tuning and regularization to ensure its applicability to a broader range of phishing scenarios. Despite these challenges, the insights gained from the ANN model are instrumental in understanding the complex, non-linear relationships in phishing data, paving the way for future advancements in this area.

The SVM model, although exhibiting a lower accuracy rate of 83.8%, provided crucial insights into the phishing strategies that require more nuanced detection approaches. This finding highlights the importance of a diverse model portfolio to address the multifaceted nature of phishing threats effectively. Incorporating user behavior and contextual data into model training and prediction is another promising avenue for paper. Techniques like behavior-based analysis or integrating contextual features from user environments could lead to more accurate and personalized phishing detection systems. This approach could enhance the models' ability to adapt to individual users' unique risk profiles and usage patterns.

Finally, addressing zero-day phishing attacks, where new and unknown threats emerge, requires models that can learn and adapt in real time. Incremental learning approaches or online learning strategies, where models update their knowledge as new data arrives, are crucial in combating these evolving threats.

In conclusion, this study has made significant strides in the use of machine learning for phishing detection. The diverse methodologies employed, the thorough dataset preparation, and the promising results all contribute to the advancement of cybersecurity measures against phishing threats. The insights gained from this paper not only underscore the potential of machine learning in this domain but also highlight the importance of continuous adaptation and improvement in the fight against cyber threats. Future paper will be pivotal in enhancing the robustness of phishing detection systems, expanding datasets, and integrating user behavior to develop more effective and personalized solutions for combating phishing attacks.

Acknowledgements

The authors would like to thank the Deanship of Graduate Studies and Scientific Research at Jouf University for funding and supporting this research through the initiative of DGSR, Graduate Students Research Support (GSR) at Jouf University, Saudi Arabia.

References

[1] A. K. Dutta, "Detecting Phishing Websites Using Machine Learning Technique," PLoS ONE, vol. 16, no. 10, e0258361, 2021. [Online]. Available: https://doi.org/10.1371/journal.pone.0258361.

[2] Jain A.K., Gupta B.B. “PHISH-SAFE: URL Features-Based Phishing Detection System Using Machine Learning”, Cyber Security. Advances in Intelligent Systems and Computing, vol. 729, 2018, https://doi.org/10.1007/978-981-10-8536-9_44

[3] Purbay M., Kumar D, “Split Behavior of Supervised Machine Learning Algorithms for Phishing URL Detection”, Lecture Notes in Electrical Engineering, vol. 683, 2021, https://doi.org/10.1007/978-981-15-6840-4_40

[4] Gandotra E., Gupta D, “An Efficient Approach for Phishing Detection using Machine Learning”, Algorithms for Intelligent Systems, Springer, Singapore, 2021, https://doi.org/10.1007/978-981-15-8711-5_12.

[5] Hung Le, Quang Pham, Doyen Sahoo, and Steven C.H. Hoi, “URLNet: Learning a URL Representation with Deep Learning for Malicious URL Detection”, Conference’17, Washington, DC, USA, arXiv:1802.03162, July 2017.

[6] Hong J., Kim T., Liu J., Park N., Kim SW, “Phishing URL Detection with Lexical Features and Blacklisted Domains”, Autonomous Secure Cyber Systems. Springer, https://doi.org/10.1007/978-3-030-33432-1_12.

[7] J. Kumar, A. Santhanavijayan, B. Janet, B. Rajendran and B. S. Bindhumadhava, “Phishing Website Classification and Detection Using Machine Learning,”

2020 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2020, pp. 1–6, 10.1109/ICCCI48352.2020.9104161.

[8] "Hassan Y.A. and Abdelfettah B, "Using case-based reasoning for phishing detection", Procedia Computer Science, vol. 109, 2017, pp. 281–288." ("[1] F. Yahya et al., Detection of Phishing Websites ... - ResearchGate")

[9] Rao RS, Pais AR. Jail-Phish: An improved search engine-based phishing detection system. Computers & Security. 2019 Jun 1; 83:246–67.

[10] "Aljofey A, Jiang Q, Qu Q, Huang M, Niyigena JP." ("Prediction of Phishing Websites Using Stacked Ensemble ... - Springer") An effective phishing detection model based on the character-level convolutional neural network from URL. Electronics. 2020 Sep; 9(9):1514.

[11] AlEroud A, Karabatis G. Bypassing detection of URL-based phishing attacks using generative adversarial deep neural networks. In: Proceedings of the Sixth International Workshop on Security and Privacy Analytics 2020 Mar 16 (pp. 53–60).

[12] R. Verma and N. Dyer, "Detection of Phishing Websites Using a Novel Twofold Ensemble Model," IEEE Access, vol. 7, pp. 114134-114145, 2019.

[13] H. R. Shahriar, M. Zulkernine, and S. M. Farhad, "PhishDef: URL names say it all," IEEE Trans. Netw. Serv. Manag., vol. 17, no. 1, pp. 498-511, Mar. 2020.

[14] B. B. Gupta, A. Tewari, D. Jain, and M. Agrawal, "Fighting against phishing attacks: state of the art and future challenges," Neural Comput. Appl., vol. 31, no. 12, pp. 9143-9169, Dec. 2020.

[15] [14] K. R. Choo, "Cryptocurrency phishing and scams: Attack vectors, impacts, and a way forward," IEEE Access, vol. 8, pp. 67512-67525, 2020.

[16] L. Zhang, S. Tan, and J. Yang, "URLNet: Learning a URL representation with deep learning for malicious URL detection," IEEE Access, vol. 8, pp. 1776-1786, 2020.

[17] M. Sharif, S. Bhagavatula, L. Bauer, and M. K. Reiter, "Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition," in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., Dallas, TX, USA, 2019, pp. 1528-1540.

[18] A. D. Nguyen, M. L. Nguyen, and N. G. Nguyen, "Deep learning for deepfakes creation and detection: A survey," IEEE Access, vol. 9, pp. 139877-139907, 2021.

[19] S. M. Al-Rawahi and M. S. Al-Fahdi, "Using machine learning techniques for rising phishing attacks on social networks," in Proc. IEEE Conf. on Application, Information and Network Security (AINS), Muscat, Oman, 2020, pp. 1-6.

[20] A. N. Khan, M. Kiah, S. A. Madani, S. Ali, and M. Shamshirband, "Phishing attacks detection using machine learning and deep learning techniques: A review," Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 6, 2019.

[21] E. Sitnikova, "Phishing in the era of advanced cyber threats," in Cybersecurity Education for Awareness and Compliance, IGI Global, 2019, pp. 28-50.