Mrs. V. Suvarna .2026, 14:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Intelligent Phishing Website Detection Using Machine Learning and URL Feature Analysis

Mrs. V. Suvarna [1] , Mallidi Mohana Sudha [2], Gunturi Satyasai Phani Amrutha Sri Varshini [3], Mungara Shakthi Indra Varma [4], Gangapatrula Ram Karthikeyan [5], Nalli Prema Chandhu [6]

[1] Assistant Professor, Department of CSE (Data Science) In Pragati Engineering College, Surampalem, Andhra Pradesh, India,
[2,3,4,5,6] UG Students Department of CSE (Data Science) In Pragati Engineering College, Surampalem, Andhra Pradesh, India.

Abstract- Phishing attacks have become one of the most common cybersecurity threats, targeting users by creating fraudulent websites that mimic legitimate platforms to steal sensitive information such as login credentials, financial data, and personal identity details. Traditional phishing detection approaches, such as blacklist-based systems and manual verification methods, are often inefficient and unable to detect newly emerging phishing websites in real time. Therefore, intelligent and automated detection mechanisms are required to improve cybersecurity and protect users from online fraud. This study proposes an efficient machine learning–based framework for detecting phishing websites using URL and domain-based features. The proposed system utilizes a dataset containing both legitimate and phishing website URLs collected from publicly available repositories. Data preprocessing techniques are applied to clean and normalize the dataset, ensuring consistency and improving model performance. Multiple machine learning algorithms including Logistic Regression, Decision Tree, Random Forest, AdaBoost, and Gradient Boosting are implemented and evaluated using stratified cross-validation techniques to ensure reliable prediction results. Among the evaluated models, ensemble learning algorithms demonstrate superior performance due to their ability to combine multiple weak learners and reduce prediction errors. In particular, the Random Forest classifier achieves high detection accuracy by analyzing key URL characteristics such as domain name structure, prefix and suffix usage, DNS records, URL length, and IP address patterns. The experimental results show that the ensemble model effectively distinguishes between legitimate and phishing websites with high accuracy, precision, recall, and F1-score.Furthermore, feature importance analysis is performed to identify the most influential attributes contributing to phishing detection, enabling better understanding of model behaviour and improving system transparency. The proposed framework provides a scalable and automated solution for detecting malicious websites, helping users identify fraudulent URLs before interacting with them. Overall, the proposed machine learning framework enhances phishing detection capability, improves cybersecurity awareness, and provides an efficient tool for protecting users against online phishing attacks.

INDEX TERMS: Phishing Website Detection, Machine Learning, Ensemble Learning, Random Forest, URL Feature Analysis, Cybersecurity, Website Security, Classification Algorithms.

I. INTRODUCTION

The rapid growth of the internet and online services has significantly increased the number of web-based transactions and digital communications across the world. While these advancements have improved convenience and accessibility, they have also created opportunities for cybercriminals to exploit online systems through various malicious activities. Among these threats, phishing attacks have emerged as one of the most common and dangerous forms of cybercrime. Phishing involves the creation of fraudulent websites or messages that imitate legitimate organizations in order to trick users into revealing sensitive information such as usernames, passwords, banking credentials, and personal identification details. These attacks pose a serious

threat to individuals, businesses, and financial institutions, leading to significant economic losses and privacy breaches.

Traditionally, phishing detection methods rely on techniques such as blacklist-based filtering, heuristic analysis, and manual inspection of suspicious URLs. Although these approaches can detect previously identified phishing websites, they are often ineffective against newly created or rapidly evolving phishing attacks. Blacklist-based systems require continuous updates and cannot detect unknown phishing websites in real time. Similarly, heuristic and rule-based detection techniques depend heavily on predefined patterns and may fail when attackers adopt new strategies to bypass security mechanisms. As phishing attacks become more sophisticated, these traditional approaches struggle to provide accurate and timely detection.

With the advancement of data-driven technologies, machine learning (ML) has emerged as a powerful solution for detecting phishing websites. Machine learning algorithms can automatically learn patterns from historical datasets and classify websites as legitimate or malicious based on various features extracted from URLs and webpage attributes. These intelligent models are capable of analyzing complex patterns within large datasets, enabling the detection of phishing attacks that may not be identifiable using conventional rule-based approaches. Machine learning techniques have been widely applied in various cybersecurity domains, including malware detection, intrusion detection systems, spam filtering, and anomaly detection, demonstrating their effectiveness in identifying hidden threats in large-scale datasets [3], [5], [7].

Despite the promising capabilities of machine learning models, several challenges remain when applying these techniques to phishing website detection. One major challenge is the dynamic nature of phishing attacks, where attackers continuously modify URLs and webpage structures to evade detection systems. In addition, phishing datasets often contain high-dimensional feature spaces and imbalanced class distributions, where the number of legitimate websites significantly exceeds the number of phishing instances. These challenges can negatively impact model performance and lead to biased predictions if not properly addressed during the training process.

To overcome these challenges, ensemble learning techniques have gained considerable attention in recent research. Ensemble methods combine the predictions of multiple machine learning models to produce more accurate and stable results compared to individual classifiers. Algorithms such as Random Forest, AdaBoost, and Gradient Boosting improve prediction accuracy by reducing bias and variance while effectively handling complex datasets. By integrating multiple weak learners into a single robust model, ensemble learning techniques provide improved classification performance for phishing detection tasks.

Motivated by these challenges, this research proposes a machine learning–based phishing website detection framework that utilizes ensemble learning techniques to identify malicious URLs. The proposed system analyses a set of URL-based and domain-based features, including URL length, prefix and suffix patterns, DNS records, IP addresses, and domain characteristics, to accurately classify websites as legitimate or phishing. By applying advanced preprocessing techniques and evaluating multiple machine learning algorithms, the framework aims to improve detection accuracy while maintaining computational efficiency.

The remainder of this paper is organized as follows. Section II presents a review of existing research related to phishing detection techniques. Section III discusses the system analysis, including the limitations of current methods and the proposed solution. Section IV describes the system architecture and methodology used for phishing detection. Section V explains the implementation modules of the proposed framework. Section VI presents the experimental results and performance evaluation of the machine learning models. Finally, Section VII concludes the study and outlines potential future improvements for enhancing phishing detection systems.

II. LITERATURE SURVEY

The rapid growth of internet usage and online services has significantly increased the occurrence of cyber threats, particularly phishing attacks. As phishing techniques continue to evolve, researchers have increasingly focused on developing intelligent detection mechanisms using machine learning and data-driven approaches. These techniques analyze patterns within large datasets and identify suspicious characteristics associated with malicious websites. With the development of modern cybersecurity infrastructures and large-scale data collection systems, machine learning-based phishing detection has become an important research area in information security and network protection systems [3], [4].

Abu-Nimeh et al. conducted an early comparative study on different machine learning algorithms for phishing detection. Their research evaluated classification techniques such as Decision Trees, Support Vector Machines, Logistic Regression, and Neural Networks to determine their effectiveness in identifying malicious websites. The study demonstrated that machine learning algorithms can significantly improve phishing detection accuracy compared to traditional rule-based approaches. However, the performance of these models depended heavily on feature selection and the quality of the training dataset.

Zuraiq and Alkasassbeh presented a comprehensive review of existing phishing detection techniques and highlighted the limitations of conventional security mechanisms. Their work emphasized that blacklist-based detection systems are incapable of identifying newly generated phishing websites because such systems rely on previously known malicious URLs. The researchers suggested that intelligent machine learning models could overcome these limitations by analyzing behavioural and structural features of URLs to detect unknown phishing attacks.
Furthermore, Basit et al. explored artificial intelligence–based approaches for phishing detection and provided an extensive survey of machine learning and deep learning techniques used in cybersecurity applications. Their study indicated that algorithms such as Random Forest, Gradient Boosting, and Neural Networks demonstrate strong performance in phishing classification tasks due to their ability to learn complex patterns from large datasets. However, they also noted that many machine learning models operate as black-box systems, making it difficult for users to understand how predictions are generated.

In another study, Arshad et al. analysed various phishing attack techniques including email spoofing, spear phishing, phone phishing, and URL manipulation. Their research highlighted that URL-based phishing attacks are particularly dangerous because attackers design fake websites that closely resemble legitimate platforms. As a result, users often fail to distinguish between genuine and malicious websites, leading to data theft and financial fraud. The authors recommended the use of intelligent detection systems capable of analyzing URL features and webpage characteristics in real time.

Catal et al. investigated the application of deep learning techniques for phishing website detection and evaluated their effectiveness using large-scale datasets. Their study demonstrated that deep learning models can achieve high detection accuracy by automatically learning feature representations from data. However, these models require significant computational resources and large training datasets, which may limit their applicability in real-time phishing detection systems.

More recently, ensemble learning techniques have gained considerable attention for improving phishing detection performance. Ensemble methods combine multiple machine learning models to produce more accurate and stable predictions. Algorithms such as Random Forest, AdaBoost, and Gradient Boosting reduce prediction errors by aggregating the outputs of multiple classifiers. Several studies have shown that ensemble models outperform individual classifiers in phishing detection tasks due to their ability to reduce bias and variance in predictions.

Despite these advancements, several challenges remain in developing efficient phishing detection systems. Phishing datasets often contain high-dimensional features and imbalanced class distributions, which can negatively affect model training and prediction accuracy. Additionally, the continuously evolving nature of phishing strategies requires detection models that can adapt to new attack patterns. Therefore, there is a need for robust machine learning frameworks that can effectively analyze URL features, improve classification accuracy, and provide reliable detection of malicious websites.

III. SYSTEM ANALYSIS

A. Existing System

Traditional phishing detection systems primarily rely on manual verification methods and rule-based security mechanisms to identify malicious websites. In these approaches, cybersecurity tools analyze website characteristics such as domain names, URL structures, and website content to determine whether a webpage is legitimate or fraudulent. One of the most widely used techniques is the blacklist-based approach, where previously identified phishing URLs are stored in a centralized database. When a user attempts to access a website, the system checks the URL against the blacklist to determine whether it has already been reported as malicious.

Although blacklist-based detection systems can successfully identify known phishing websites, they are ineffective in detecting newly generated or previously unseen phishing URLs. Cyber attackers continuously modify their phishing techniques by changing domain names, URL structures, and website designs to bypass security mechanisms. As a result, traditional blacklist systems fail to provide real-time protection against emerging phishing threats.

Another commonly used method is heuristic-based detection, which analyses predefined rules related to URL patterns and webpage features. These rules may include identifying suspicious characteristics such as unusually long URLs, excessive use of special characters, or domain names that closely resemble legitimate websites. While heuristic approaches can detect certain phishing attempts, they often generate high false-positive rates and struggle to adapt to new phishing strategies.

With the advancement of artificial intelligence and machine learning technologies, researchers have introduced machine learning-based phishing detection models that learn patterns from historical datasets. These models use classification algorithms such as Logistic Regression, Decision Trees, Support Vector Machines (SVM), and Neural Networks to differentiate between legitimate and phishing websites. By analyzing features extracted from URLs, domain information, and webpage content, machine learning models can identify suspicious patterns that indicate phishing activity.

Furthermore, ensemble learning algorithms such as Random Forest, AdaBoost, and Gradient Boosting have been widely adopted to improve detection accuracy and robustness. These algorithms combine multiple weak classifiers to produce a stronger predictive model, thereby reducing prediction errors and improving overall classification performance [5], [7]. Despite these improvements, several challenges remain in developing efficient phishing detection systems.

Recent advancements in web technologies have also enabled the integration of real-time monitoring systems capable of analyzing large volumes of web traffic and user interaction data. These systems collect extensive datasets containing both legitimate and phishing URLs, which can be used to train machine learning models. However, many existing detection systems rely on complex models that behave as black-box algorithms, making it difficult to interpret their predictions and understand how specific features influence classification results [8], [11].

To address this challenge, researchers have introduced Explainable Artificial Intelligence (XAI) techniques that improve the transparency of machine learning models. Methods such as SHAP (SHapley Additive Explanations) and LIME (Local

Interpretable Model-Agnostic Explanations) help explain the contribution of individual features to prediction outcomes. These techniques enhance trust and reliability in AI-based cybersecurity systems by allowing analysts to understand the reasoning behind model predictions [1], [2], [9], [12].

Limitations Of Existing System

Despite the advancements in phishing detection technologies, several limitations still exist in current systems:

Inability to Detect Newly Generated Phishing Websites:
Blacklist-based systems depend on previously identified malicious URLs and therefore fail to detect newly created phishing websites that are not yet included in the database.

High False Positive and False Negative Rates:
Heuristic-based detection methods rely on predefined rules that may incorrectly classify legitimate websites as phishing or fail to detect sophisticated phishing attacks.

Dynamic Nature of Phishing Attacks:
Phishers frequently modify website structures, domain names, and URL patterns to bypass existing detection systems, making it difficult for static detection models to adapt to evolving threats.

High-Dimensional Feature Complexity:
Phishing detection datasets often contain numerous URL and domain-related features, which can increase computational complexity and negatively impact model training efficiency.

Lack of Model Interpretability:
Many advanced machine learning algorithms operate as black-box models, making it difficult for cybersecurity experts to understand how predictions are generated and which features influence the detection process.

Dataset Imbalance Issues:
In most phishing detection datasets, legitimate websites significantly outnumber phishing websites. This imbalance may cause machine learning models to become biased toward the majority class, reducing detection performance for malicious websites.

Due to these challenges, there is a need for an intelligent phishing detection system that can effectively analyze URL-based features, handle dataset imbalances, and provide accurate classification while maintaining computational efficiency and transparency.

B. Proposed System
To address the limitations of existing phishing detection approaches, this research proposes a machine learning–based phishing website detection framework that utilizes ensemble learning techniques for improved accuracy and reliability. The proposed system analyses various URL-based and domain-based features to determine whether a website is legitimate or malicious.

The framework begins with collecting a dataset containing both phishing and legitimate website URLs from publicly available repositories. Data preprocessing techniques are applied to clean the dataset, remove missing values, and normalize feature distributions to improve the performance of machine learning algorithms.

After preprocessing, several machine learning classification models are implemented, including Logistic Regression, Decision Tree, Random Forest, AdaBoost, and Gradient Boosting. These algorithms are trained using historical URL datasets to learn patterns associated with phishing websites. Among these models, ensemble learning techniques such as Random Forest provide improved prediction accuracy by combining multiple decision trees and reducing prediction variance.

The proposed system extracts several important features from URLs, including domain name characteristics, URL length, prefix and suffix patterns, DNS record information, and IP address usage. These features help the model identify suspicious patterns commonly associated with phishing websites.

The trained machine learning model is integrated into a web-based application that allows users to input a URL for analysis. When a user submits a URL, the system extracts relevant features, processes the data, and predicts whether the website is legitimate or phishing. The prediction result is displayed to the user in real time, enabling them to make informed decisions before accessing potentially harmful websites.

By combining feature engineering, ensemble learning algorithms, and automated classification techniques, the proposed framework aims to improve phishing detection accuracy while maintaining system efficiency. This approach enhances cybersecurity by providing users with an intelligent tool capable of detecting fraudulent websites and preventing online data theft.

IV. SYSTEM DESIGN

System Architecture

Below diagram depicts the whole system architecture.

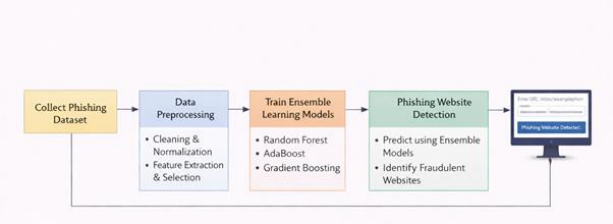

Fig 1. Methodology followed for proposed model

V. SYSTEM IMPLEMENTATION

Modules

This section describes the implementation modules of the proposed machine learning framework developed for phishing website detection. The system follows a structured pipeline that includes dataset collection, data preprocessing, feature extraction, machine learning model training, and phishing website prediction. This modular architecture improves the scalability, reliability, and performance of the detection system while enabling efficient identification of fraudulent websites.

A. Data Collection Module

The Data Collection Module is responsible for gathering datasets containing both legitimate and phishing website URLs. These datasets are typically obtained from publicly available cybersecurity repositories such as phishing databases and website security research platforms. The collected dataset contains several attributes related to URL characteristics, domain information, and webpage features. These attributes include parameters such as URL length, presence of special characters, domain registration details, SSL certificate usage, and redirection behavior. Each URL in the dataset is labelled as either phishing or legitimate, enabling supervised learning for classification. The dataset reflects real-world cybersecurity scenarios where phishing websites attempt to mimic legitimate websites to deceive users and steal sensitive information such as login credentials, banking details, and personal data. Because phishing URLs are often fewer than legitimate URLs, the dataset may exhibit class imbalance. The collected dataset is stored in a structured format and forwarded to the preprocessing module for further analysis.

B. Data Preprocessing Module

The Data Preprocessing Module prepares the dataset for machine learning model training by improving data quality and removing inconsistencies. Real-world cybersecurity datasets may contain missing values, noisy data, or inconsistent feature distributions that can negatively affect model performance.

The preprocessing stage consists of several steps:

1) Data Cleaning

Irrelevant or duplicate entries are removed from the dataset to ensure consistency and reliability. Missing values are identified and handled appropriately to prevent errors during model training.

2) Feature Normalization

Feature scaling techniques are applied to normalize the range of input features. This ensures that all features contribute equally during the training process and prevents bias caused by different numerical scales.

3) Dataset Balancing

In phishing detection datasets, legitimate URLs typically outnumber phishing URLs. To address this imbalance, techniques such as Synthetic Minority Oversampling Technique (SMOTE) can be used to generate synthetic phishing samples and improve model learning performance.

These preprocessing steps enhance dataset quality and ensure that machine learning models can learn meaningful patterns for accurate phishing detection.

C. Feature Extraction and Selection Module

Phishing detection relies heavily on analyzing various URL-based and domain-based features. The Feature Extraction Module identifies important attributes from the collected dataset that contribute to distinguishing phishing websites from legitimate ones.

Some commonly extracted features include:

- URL length
- Presence of special characters in URL
- Use of IP address instead of domain name
- Domain age and registration information
- HTTPS protocol usage
- Number of subdomains
- URL redirection behavior

After extracting these attributes, the Feature Selection Module evaluates their importance using machine learning techniques. Feature importance can be estimated using tree-based algorithms or explainability methods such as SHAP (SHapley Additive Explanations).Selecting the most relevant features reduces dataset dimensionality, decreases computational complexity, and improves model interpretability while maintaining high predictive accuracy [1], [2], [8].

D. Machine Learning Training Module

The Machine Learning Training Module builds classification models that predict whether a given website URL is phishing or legitimate. Several supervised machine learning algorithms are implemented and evaluated during the training process.

The algorithms used in this study include:

- Logistic Regression
- Decision Tree
- Support Vector Machine (SVM)
- Gradient Boosting
- Random Forest

Each model is trained using the pre-processed dataset containing labelled phishing and legitimate URLs. To ensure reliable performance evaluation, the dataset is divided into training and testing sets, and stratified cross-validation is applied to maintain balanced class distribution.

Among the evaluated models, ensemble learning techniques such as Random Forest and Gradient Boosting often provide higher accuracy and improved generalization performance. Random Forest, in particular, combines multiple decision trees to produce stable predictions while reducing overfitting and improving classification reliability [5], [7].

E. Prediction and Detection Module

The Prediction Module performs the final classification of websites using the trained machine learning model. When a user inputs a website URL into the system, the following steps are performed:

1. The URL is analysed and relevant features are extracted.
2. The extracted features are processed using the trained machine learning model.
3. The system predicts whether the website is legitimate or phishing.

The output of the system includes:

- Website classification result (Phishing / Legitimate)
- Prediction probability score
- Risk indication for user awareness

F. Model Evaluation Module

To evaluate the performance of the phishing detection system, several classification performance metrics are used:

- Accuracy – measures overall classification correctness
- Precision – measures the proportion of correctly detected phishing websites
- Recall – measures the system's ability to detect phishing attacks
- F1-Score – harmonic mean of precision and recall
- ROC–AUC Score – evaluates the model's ability to distinguish between phishing and legitimate websites

These evaluation metrics provide a comprehensive assessment of the model's effectiveness, particularly in cybersecurity applications where detecting rare phishing attacks is critically important. By accurately identifying malicious websites before users access them, the proposed phishing detection framework enhances online security, prevents data theft, and reduces the risk of financial fraud in digital environments.

VI. RESULTS AND DISCUSSION

This section presents the experimental results and performance evaluation of the proposed machine learning framework for detecting phishing websites. Multiple classification algorithms were trained and evaluated using a labelled dataset containing both legitimate and phishing URLs. The evaluation focuses on comparing model performance, analyzing prediction accuracy, and examining the importance of features used for phishing detection. The machine learning models were trained using stratified cross-validation to maintain the distribution of phishing and legitimate samples across training and testing datasets. Several performance metrics such as accuracy, precision, recall, and F1-score were used to evaluate the effectiveness of the models.

A. Accuracy Comparison of Machine Learning Models

Several machine learning algorithms were implemented to determine the most suitable model for phishing website detection. The evaluated models include Logistic Regression, Decision Tree, Support Vector Machine (SVM), Gradient Boosting, and Random Forest.

Model performance was assessed using multiple classification metrics to ensure a comprehensive evaluation of detection capability.

Table 1. Performance Comparison of Machine Learning Models

Model	**Accuracy (%)**	**Precision**	**Recall**	**F1-Score**
Logistic Regression	88.2	0.87	0.85	0.86
Decision Tree	90.1	0.89	0.88	0.88
Support Vector Machine	91.6	0.90	0.90	0.90
Gradient Boosting	94.2	0.93	0.92	0.92
Random Forest	96.1	0.95	0.94	0.94

From the comparison results, the Random Forest classifier achieved the highest accuracy of 96.1%, outperforming other machine learning algorithms. This improved performance is mainly attributed to its ensemble learning mechanism, which combines multiple decision trees to produce more stable and reliable predictions. Ensemble learning methods effectively reduce overfitting and improve classification robustness, particularly in cybersecurity datasets where patterns can be highly complex [5], [7].

The results demonstrate that ensemble-based models provide better generalization capability and

higher detection accuracy compared to individual classifiers.

B. Roc Curve Analysis

The Receiver Operating Characteristic (ROC) curve is widely used to evaluate the trade-off between the True Positive Rate (TPR) and False Positive Rate (FPR) at various classification thresholds. The Area Under the Curve (ROC–AUC) metric represents the ability of a classifier to distinguish between phishing and legitimate websites.

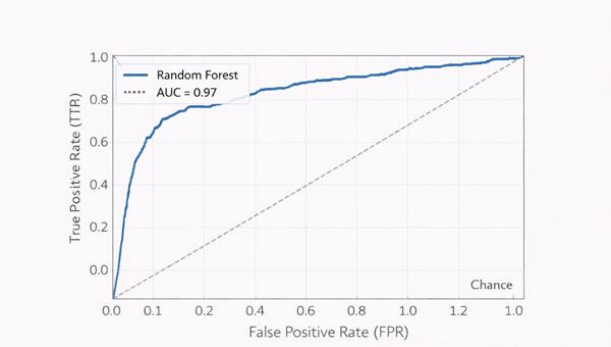

Fig. 2. ROC Curve for Phishing Website Detection Model

The ROC curve analysis shows that the Random Forest classifier achieved a ROC–AUC score of 0.97, indicating excellent classification capability. A ROC curve that approaches the top-left corner of the graph suggests that the model effectively minimizes false positives while maximizing the detection of phishing websites.

This result demonstrates that the proposed framework can accurately detect phishing attacks even when the dataset contains imbalanced classes, which is a common characteristic of cybersecurity datasets.

C. Feature Importance Analysis

To improve transparency and interpretability of the phishing detection model, feature importance analysis was performed using SHAP (SHapley Additive Explanations). SHAP values provide insights into how individual features contribute to the prediction outcome by estimating the impact of each feature on the classification decision.

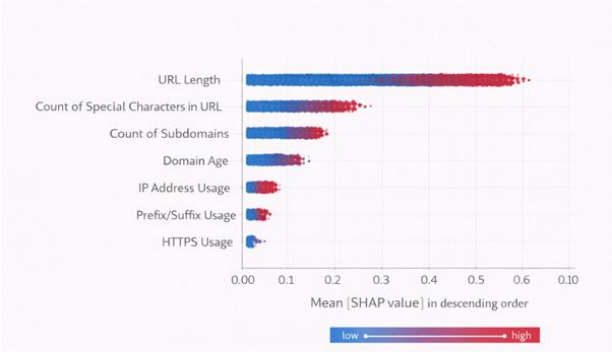

Fig. 3. Feature Importance for Phishing Website Detection

The SHAP analysis revealed that several URL-based attributes significantly influence phishing detection. The most important features include:

- URL length
- Presence of special characters in the URL
- Number of subdomains
- Domain age
- Use of IP address instead of domain name
- HTTPS protocol usage

Features with higher SHAP values contribute more strongly to the model's prediction decision. For example, unusually long URLs or URLs containing excessive special characters often indicate suspicious or malicious websites. The global SHAP summary plot illustrates the relative importance of different features across the entire dataset, while local SHAP explanations provide insights into how specific features influence individual predictions. The integration of explainable AI techniques enhances the interpretability of the phishing detection system and allows cybersecurity analysts to understand how the machine learning model identifies malicious websites. This transparency improves trust and reliability in AI-based security systems [1], [2], [8], [12].

VII. CONCLUSION AND FUTURE WORK

This study proposed a machine learning–based framework for detecting phishing websites using

URL-based and domain-based features. Phishing attacks continue to be one of the most significant cybersecurity threats, as attackers frequently create fraudulent websites that imitate legitimate services to steal sensitive user information. To address this challenge, the proposed system utilizes supervised machine learning techniques to automatically classify websites as legitimate or phishing based on various extracted features.

The dataset used in this study contained multiple attributes related to URL structure, domain information, and webpage characteristics. Because phishing datasets often contain imbalanced distributions between legitimate and malicious websites, appropriate preprocessing techniques were applied to improve model training and prediction reliability. Data cleaning, normalization, and feature extraction methods were implemented to enhance dataset quality and improve model performance.

Several machine learning algorithms were evaluated, including Logistic Regression, Decision Tree, Support Vector Machine, Gradient Boosting, and Random Forest. Among these models, the Random Forest classifier achieved the highest detection accuracy of approximately 96%, demonstrating strong capability in identifying phishing websites. The ensemble learning mechanism of Random Forest improves prediction stability by combining multiple decision trees, thereby reducing overfitting and increasing classification robustness in cybersecurity datasets [5], [7].

In addition, Explainable Artificial Intelligence (XAI) techniques such as SHAP (SHapley Additive Explanations) were applied to analyze the importance of features used in phishing detection. The explainability analysis revealed that features such as URL length, number of subdomains, special characters in URLs, domain age, and HTTPS usage significantly influence phishing classification decisions. Integrating explainability techniques improves transparency and helps cybersecurity analysts better understand how machine learning models detect malicious websites [1], [2], [8], [12].

Overall, the proposed framework demonstrates that machine learning techniques can effectively detect phishing websites and improve online security by providing automated and reliable classification mechanisms. Future work may focus on integrating real-time phishing detection systems within web browsers or security gateways, enabling continuous monitoring of website activity. In addition, advanced deep learning techniques such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and transformer-based architectures may be explored to further improve detection accuracy. Furthermore, incorporating large-scale real-time datasets and adaptive learning mechanisms could enhance the system's ability to detect emerging phishing strategies and evolving cyber threats.

REFERENCES

1. M. Qabajeh, F. Thabtah, and F. Chiclana, "Conventional vs. automated phishing detection techniques," in Proc. 1st Babylon Int. Conf. Information Technology and Science (BICITS), Apr. 2012, pp. 41–45.
2. M. Zuraiq and M. Alkasassbeh, "Comprehensive review of current phishing detection methods," Proc. Inst. Mech. Eng. Part D: Journal of Automobile Engineering, vol. 229, no. 2, pp. 163–173, 2015.
3. S. Kunju, R. Thomas, and M. Joseph, "Survey method to detect phishing attacks," IFAC-PapersOnLine, vol. 54, no. 15, pp. 526–531, 2021.
4. V. Benevides, R. M. Silva, and A. F. B. Costa, "A systematic review of deep learning approaches for phishing detection," in Computer Vision and Image Processing (Communications in Computer and Information Science), N. Nain and S. K. Vipparthi, Eds. Cham, Switzerland: Springer, 2020.
5. P. Athulya and C. Praveen, "Different phishing attacks, recent phishing tactics, and anti-phishing strategies," in Proc. Asian Conf. Computer Vision, Lecture Notes in Computer Science, C.-S. Chen, J. Lu, and K.-K. Ma, Eds. Cham, Switzerland: Springer, 2020, pp. 154–164.
6. A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, "A survey of artificial intelligence-based phishing detection techniques," IEEE

Transactions on Intelligent Transportation Systems, vol. 18, no. 3, pp. 545–557, Mar. 2020.
7. K. Kathrine, S. Rahman, and M. Hossain, "A framework to detect and prevent different types of phishing attacks," CoRR, vol. abs/1801.02325, 2019.
8. E. Korkmaz, "A review for selecting features used in URL-based phishing detection systems," in Proc. Int. Conf. Omni-Layer Intelligent Systems (COINS), Aug. 2020, pp. 1–8.
9. S. Arshad, M. A. Shah, and A. Khan, "Phishing attack detection techniques and analysis of phishing methods," IEEE Access, vol. 8, pp. 207545–207556, 2021.
10. C. Catal, B. Tekinerdogan, and O. Ozcan, "Deep learning approaches for phishing detection: A systematic review," Future Generation Computer Systems, vol. 131, pp. 151–165, Jun. 2022.
11. A. Lakshamanarao, P. S. P. Rao, and M. M. B. Krishna, "Phishing website detection using a novel machine learning fusion approach," in Proc. Int. Conf. Artificial Intelligence and Smart Systems (ICAIS), 2021, pp. 1164–1169.
12. D. Vaishnavi, S. Suwetha, Y. B. Jinila, R. Subhashini, and S. P. Shyry, "Comparative analysis of machine learning algorithms for malicious URL prediction," in Proc. 5th Int. Conf. Intelligent Computing and Control Systems (ICICCS), 2021, pp. 1398–1402.
13. S. Abu-Nimeh, D. Nappa, X. Wang, and S. Nair, "A comparison of machine learning techniques for phishing detection," in Proc. Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit, 2007.
14. B. E., K. T., and T. K., "Phishing URL detection: A machine learning and web mining-based approach," International Journal of Computer Applications, vol. 123, no. 13, pp. 46–50, 2015.