Classification Of Features for Detecting Phishing Web Sites Based on Machine Learning Techniques

Annappa S S[1], Asha S[2]
[1,2]*Sahyadri Science College*

***Abstract*—Phishing is one of the most widespread forms of cybercrime and poses a significant threat to individuals and organizations by attempting to steal sensitive information such as usernames, passwords, banking credentials, credit card details, and personal identification data. Attackers typically create fraudulent websites that closely resemble legitimate ones, misleading users into revealing confidential information. As phishing techniques continue to evolve, developing an effective and reliable detection mechanism remains a challenging task due to the dynamic nature of website characteristics and attack strategies. This study focuses on the detection of phishing websites using machine learning techniques. The proposed approach utilizes the Phishing Websites dataset available from the UCI Machine Learning Repository, which consists of 30 website-related features representing various characteristics of web pages. These features are analyzed to distinguish phishing websites from legitimate ones. To improve phishing detection, an Extreme Learning Machine (ELM) classifier is employed and its performance is evaluated against other well-known machine learning algorithms, including Naïve Bayes (NB) and Artificial Neural Networks (ANN). Experimental results demonstrate that the ELM-based model achieves superior classification performance, attaining an accuracy of 89.3%, thereby outperforming the comparative methods. The findings indicate that machine learning techniques, particularly Extreme Learning Machine, provide an efficient and practical solution for identifying phishing websites and enhancing cybersecurity.**

***Index Terms*—Extreme Learning Machine (ELM), Phishing Website Detection, Machine Learning, Information Security, Cybersecurity, Feature Classification, Website Classification, UCI Machine Learning Repository.**

I. INTRODUCTION

The rapid growth of internet-based services has significantly improved communication, online banking, e-commerce, and digital transactions. However, this increased dependence on web applications has also created opportunities for cybercriminals to exploit users through various online attacks. Among these threats, phishing remains one of the most prevalent and damaging cyberattacks, as it aims to obtain confidential information by impersonating legitimate websites and online services. Phishing attacks typically involve the creation of counterfeit web pages that closely resemble authentic websites in terms of appearance, layout, and functionality. Unsuspecting users are persuaded to visit these fraudulent websites through deceptive emails, instant messages, social media posts, advertisements, or malicious hyperlinks. Once users enter sensitive information such as login credentials, banking details, credit card numbers, or personal identification information, the attackers capture and misuse the data for financial fraud or identity theft.

Modern phishing campaigns employ a combination of technical manipulation and social engineering techniques to increase their effectiveness. Since phishing websites are designed to imitate genuine websites with high accuracy, even users with adequate cybersecurity awareness may find it difficult to distinguish legitimate websites from malicious ones. Furthermore, attackers continuously modify their strategies, making phishing detection a challenging task for traditional security mechanisms.

Several approaches have been proposed to reduce phishing attacks, including user awareness programs, legal regulations, browser-based security tools, blacklisting techniques, and machine learning-based detection systems. Among these, machine learning has emerged as a promising solution because it can automatically identify hidden patterns and classify websites based on their characteristics without relying

solely on predefined rules or manually maintained blacklists.

In this work, an Extreme Learning Machine (ELM)-based phishing website detection model is presented using the Phishing Websites dataset from the UCI Machine Learning Repository. The dataset consists of 30 website-related features that describe different characteristics of web pages. The performance of the proposed model is evaluated and compared with other classification techniques such as Naïve Bayes (NB) and Artificial Neural Networks (ANN). Experimental results demonstrate that the ELM classifier provides effective phishing website detection with improved classification accuracy, making it a suitable approach for enhancing web security.

II. RELATED WORK

To improve phishing prevention, researchers introduced hyperlink verification techniques such as the LinkGuard algorithm. This approach analyzes hyperlinks by comparing the visible URL with the actual destination URL, validating DNS information, identifying hexadecimal or dotted-decimal IP addresses, detecting encoded links, and applying pattern-matching rules. While LinkGuard effectively detects many malicious links, it may incorrectly classify legitimate websites that use IP addresses instead of registered domain names. In addition, the algorithm may generate false-negative results when users have not previously visited or verified the genuine website.

URL-based phishing detection has also received considerable attention. Garera et al. proposed a Logistic Regression model that classifies phishing URLs using manually selected lexical and statistical features. Their feature set includes suspicious keywords within URLs, Google PageRank information, and webpage quality indicators. The study demonstrated that carefully selected URL features significantly improve phishing detection; however, direct comparison with other approaches is difficult because different datasets and feature extraction methods are often used.

III. MATH

The phishing website dataset used in this study consists of *30 carefully selected features* that describe the characteristics of URLs, domain information, and webpage content. These features help distinguish legitimate websites from phishing websites by analyzing structural, lexical, and security-related properties. Based on predefined decision rules, each feature contributes to the classification process. The important features used in this research are described below. ### Feature 1: Presence of IP Address Legitimate websites generally use registered domain names instead of numerical IP addresses. Attackers often hide the actual destination by embedding an IP address, sometimes encoded in hexadecimal or other formats, directly within the URL.

Rule: ** * IP address present in the URL → **Phishing * Domain name present → **Legitimate** ### Feature 2: URL Length The length of a URL is an important indicator of phishing activity. Fraudulent websites often contain unusually long URLs to conceal malicious content or imitate legitimate websites. **Rule: ** * URL length < 54 characters → **Legitimate** * URL length between 54 and 75 characters → **Suspicious** * URL length > 75 characters → **Phishing** ### Feature 3: URL Shortening Services URL shortening services such as TinyURL are frequently used to hide the actual destination of a webpage, making it difficult for users to identify malicious links. **Rule: ** * Shortened URL detected → **Phishing** * Otherwise → **Legitimate** ### Feature 4: Use of '@' Symbol in URLs, everything preceding the '@' symbol is ignored by most web browsers. Attackers exploit this behavior to deceive users by displaying misleading addresses. **Rule: ** * '@' symbol present → **Phishing** * Otherwise → **Legitimate** ### Feature 5: Redirect Using "//" Multiple occurrences of the "//" symbol beyond the protocol portion of the URL may indicate redirection to another malicious website. **Rule: ** * Last occurrence of "//" appears after the seventh position → **Phishing** * Otherwise → **Legitimate** ### Feature 6: Hyphen (-) in Domain Name Phishing domains frequently include hyphens to imitate trusted domain names or create visually similar website addresses. **Rule: ** * Hyphen present in the domain name → **Phishing** * Otherwise → **Legitimate** ### Feature 7: Number of Subdomains The number of subdomains is used to estimate the authenticity of a website. Excessive subdomains are commonly associated with phishing

websites. **Rule: ** * One subdomain → **Legitimate** * Two subdomains → **Suspicious** * More than two subdomains → **Phishing** ### Feature 8: HTTPS and SSL Certificate Secure websites generally use HTTPS with valid SSL certificates issued by trusted Certificate Authorities. Certificate validity also contributes to website authenticity. **Rule: ** * HTTPS enabled with a trusted certificate valid for one year or more → **Legitimate** * HTTPS with an untrusted certificate → **Suspicious** * No valid HTTPS protection → **Phishing** ### Feature 9: Domain Registration Period Phishing websites are usually registered for short durations, whereas legitimate websites often maintain long-term domain registrations. **Rule: ** * Domain registration period ≤ 1 year → **Phishing** * Domain registration period > 1 year → **Legitimate** ### Feature 10: Favicon Source A favicon loaded from a domain different from the webpage's primary domain may indicate a fraudulent website attempting to imitate another site. **Rule: ** * Favicon loaded from an external domain → **Phishing** * Otherwise → **Legitimate** ### Feature 11: Standard Port Usage Legitimate websites typically operate using standard network ports. The use of unusual or unauthorized ports may indicate suspicious server configurations. **Rule: ** * Standard service ports used → **Legitimate** * Unusual or insecure port configuration → **Suspicious/Phishing** ### Feature 12: HTTPS Token in Domain Name Attackers sometimes include the term "HTTPS" within the domain name to create a false impression of security. **Rule: ** * "HTTPS" token present in the domain name → **Phishing** * Otherwise → **Legitimate** ### Feature 13: Request URL Legitimate webpages generally load embedded resources such as images, scripts, and multimedia files from the same domain. A large number of external resource requests may indicate phishing behavior. **Rule:** * Majority of resources loaded from the same domain → **Legitimate** * Large proportion of resources loaded from external domains → **Phishing** The remaining features in the UCI phishing dataset evaluate additional webpage characteristics, including anchor URLs, links in HTML tags, form handling, email submission, abnormal URLs, website forwarding, status bar customization, disabling right-click functionality, pop-up windows, iframe usage, domain age, DNS records, web traffic, page ranking, Google indexing, and inbound links. Together, these 30 features provide a comprehensive representation of website behavior and improve the effectiveness of machine learning models for phishing website detection.

IV. METODOLOGY

The proposed phishing website detection system evaluates the performance of three supervised machine learning algorithms: Artificial Neural Network (ANN), Naïve Bayes (NB), and Extreme Learning Machine (ELM). Each classifier is trained using the extracted website features from the UCI Phishing Websites dataset and is evaluated based on its classification accuracy.

A. Artificial Neural Network (ANN)

Artificial Neural Network (ANN) is a supervised learning model inspired by the biological neural system. It consists of an input layer, one or more hidden layers, and an output layer. The network learns the relationship between input features and output classes by adjusting connection weights during the training process.

The performance of an ANN depends on several design parameters, including the number of hidden layers, the number of neurons in each layer, learning rate, momentum, and the number of training epochs. Selecting these parameters is a challenging task and often requires multiple experiments to obtain an optimal network architecture.

Algorithm

1. Initialize the connection weights and bias values randomly.
2. Feed the training samples into the input layer.
3. Compute the activation values of the hidden neurons using the selected activation function.
4. Generate the output values from the output layer.
5. Calculate the error by comparing the predicted output with the target class.
6. Propagate the error backward through the network.
7. Update the connection weights using the backpropagation learning algorithm.
8. Repeat the process until the error reaches a predefined threshold or the maximum number of training iterations is completed.

Classification Accuracy: 87.901%

B. Naïve Bayes (NB)

Naïve Bayes is a probabilistic classification algorithm based on Bayes' theorem. It assumes that all input features are conditionally independent given the class label.

Although this assumption is often not strictly satisfied in real-world datasets, the algorithm is computationally efficient and performs well for many classification problems.

For continuous-valued attributes, the Gaussian Naïve Bayes model is commonly employed, where feature values are assumed to follow a normal distribution.

Algorithm

1. Collect and preprocess the training dataset.
2. Estimate the prior probability for each class.
3. Calculate the likelihood of every feature using the Gaussian probability distribution.
4. Compute the posterior probability for each class using Bayes' theorem:

[P(C|X) =\frac{P(X|C) \times P(C)} {P(X)}]

where:

- (P(C|X)) is the posterior probability,
- (P(X|C)) is the likelihood,
- (P(C)) is the prior probability,
- (P(X)) is the evidence.

5. Assign the sample to the class having the highest posterior probability.

Classification Accuracy: 61.365%

C. Extreme Learning Machine (ELM)

Extreme Learning Machine (ELM) is a fast-learning algorithm for Single Hidden Layer Feedforward Neural Networks (SLFNs). Unlike conventional neural networks, ELM randomly initializes the hidden layer parameters and computes the output weights analytically without iterative weight updates. This significantly reduces training time while maintaining high classification performance.

The hidden layer parameters remain fixed throughout the learning process, and only the output weights are determined using a least-squares solution.

Because of its simple architecture and rapid convergence, ELM has become an effective classifier for phishing website detection.

Algorithm

1. Randomly initialize the input weights and hidden-layer bias values.
2. Compute the hidden-layer output matrix using the selected activation function.
3. Calculate the Moore–Penrose pseudoinverse of the hidden-layer output matrix.
4. Determine the output weight matrix analytically.
5. Use the trained ELM model to classify unseen website samples as phishing or legitimate.

The mathematical representation of the output weight matrix is given by:

[beta=H^{\dagger} T]

where:

- (H) represents the hidden-layer output matrix,
- (H^{\dagger}) denotes the Moore–Penrose pseudoinverse of (H),
- (T) is the target output matrix,
- (\beta) is the output weight matrix.

Classification Accuracy: 89.300%

Performance Comparison

The experimental evaluation shows that the Extreme Learning Machine outperforms both Artificial Neural Network and Naïve Bayes in terms of classification accuracy. While ANN provides competitive performance, it requires iterative training and careful parameter tuning. Naïve Bayes offers fast computation but is limited by its independence assumption. ELM combines rapid training with superior predictive accuracy, making it the most effective classifier among the three algorithms for phishing website detection.

V. HELPFUL HINTS

As observed extreme leaning machine acquires the highest measurable values when compared to others.

Table I presents the comparative performance of the three machine learning algorithms—Artificial Neural Network (ANN), Naïve Bayes (NB), and Extreme Learning Machine (ELM). The evaluation is based on four standard performance metrics: Precision, Recall, F1-Score, and Accuracy. These metrics are used to assess the effectiveness of each classifier in identifying phishing websites and distinguishing them from legitimate websites.

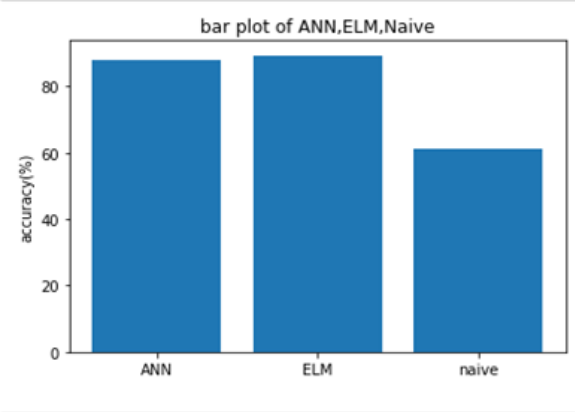

Fig. 1. Graph to show accuracy for three algorithms

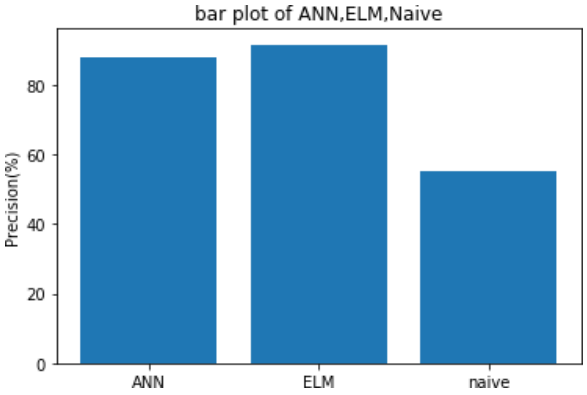

Fig. 2. Graph to show precision for three algorithms

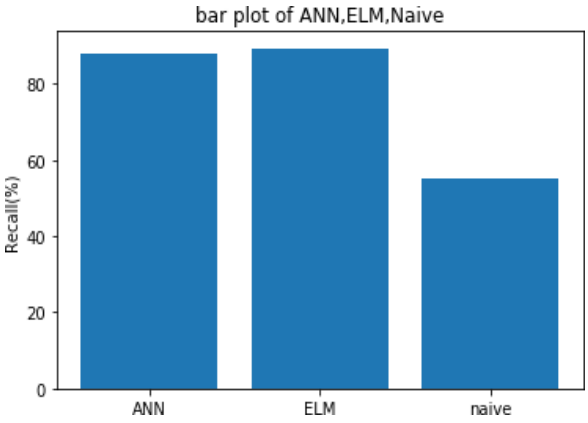

Fig.3 Graph to show f1score for three algorithms

ML Techniques	Precision (%)	Recall (%)	F1score (%)	Accuracy (%)
Naive Bayes	55.6	55.5	55.6	61.3
ANN	89.3	89.3	89.3	87.9
ELM	91.5	89.3	90.4	89.3

Accuracy and f1 score for ELM Activation Functions

Table II. The below table shows the accuracy and f1score for each of the activation functions of ELM

Measures	Accuracy	F1score
Sigmoid	89.1	89.9
Tanh	90.2	89.2
Sine	56.4	61.6
Tribas	66.4	70.3
Multiquadric	83.0	84.5
Inv_tribas	66.2	72.5
Inv_multiquadric	72.8	82.3
Hardlim	84.2	86.9
Softlim	89.3	88.3
Gaussian	71.2	75.6

VI. CONCLUSION

Phishing websites continue to pose a major cybersecurity challenge by deceiving users into disclosing sensitive information such as login credentials, banking details, and personal identification data. Detecting these fraudulent websites at an early stage is essential to protect users and maintain the security of online services.

In this study, a machine learning-based phishing website detection system was developed using the UCI Phishing Websites dataset containing 30 website-related features and one class label. The dataset was used to train and evaluate three classification algorithms: Naïve Bayes (NB), Artificial Neural Network (ANN), and Extreme Learning Machine (ELM). The performance of these models was assessed using standard evaluation metrics, including Precision, Recall, F1-Score, and Accuracy.

Experimental results indicate that the Extreme Learning Machine (ELM) classifier outperformed the other methods, achieving an accuracy of 89.3%, a precision of 91.5%, a recall of 89.3%, and an F1-score of 90.4%. ANN also produced competitive results, whereas Naïve Bayes showed comparatively lower classification performance. The findings demonstrate that ELM provides faster learning and more effective classification for phishing website detection.

The proposed approach confirms that machine learning techniques can successfully identify phishing websites using URL and webpage features. In future work, the detection performance can be further improved by incorporating additional real-time

website features, feature selection techniques, and advanced deep learning models. Furthermore, evaluating the proposed model on larger and more recent phishing datasets may improve its robustness and applicability in real-world cybersecurity environments.

APPENDIX

Appendixes, if needed, appear before the acknowledgment.

ACKNOWLEDGMENT

The authors, Annappa S. S. and Asha S, sincerely acknowledge their own efforts, dedication, and collaboration in completing this research work. This study was carried out independently.

REFERENCES

[1] P. Ying and D. Xuhua, "Anomaly based web phishing page detection," in *Proc. Annu. Comput. Security Appl. Conf. (ACSAC)*, 2006, pp. 381–390.
[2] M. Moghimi and A. Y. Varjani, "New rule-based phishing detection method," Expert Syst. Appl., vol. 53, pp. 231–242, 2016.
[3] M. Lichman, "UCI Machine Learning Repository," School of Information and Computer Science, University of California, Irvine, CA, USA, 2013. [Online]. Available: http://archive.ics.uci.edu/ml
[4] G.-B. Huang, Q.-Y. Zhu, and C.-K. Siew, "Extreme learning machine: Theory and applications," Neurocomputing, vol. 70, nos. 1–3, pp. 489–501, 2006.
[5] G.-B. Huang, Q.-Y. Zhu, and C.-K. Siew, "Extreme learning machine: A new learning scheme of feedforward neural networks," in Proc. Int. Joint Conf. Neural Netw. (IJCNN), 2004, pp. 985–990.
[6] T. S. Guzella and W. M. Caminhas, "A review of machine learning approaches to spam filtering," Expert Syst. Appl., vol. 36, no. 7, pp. 10206–10222, 2009.
[7] W. D. Yu, S. Nargundkar, and N. Tiruthani, "A phishing vulnerability analysis of web-based systems," in Proc. IEEE Symp. Comput. Commun. *(ISCC)*, 2008, pp. 326–331.