A Lightweight Comparative Machine Learning Framework for Phishing Website Detection Using Optimized URL Features

Priya Pal , Vivek Shukla , Atul * , Divya Mishra , Rishabh Tiwari , Mehul Kumar Das

Posted Date: 26 May 2026

doi: 10.20944/preprints202605.1680.v1

Keywords: phishing detection; machine learning; URL features; cybersecurity; random forest; lightweight detection

 doi:10.20944/preprints202605.1680.v1

Article

A Lightweight Comparative Machine Learning Framework for Phishing Website Detection Using Optimized URL Features

Priya Pal, Vivek Shukla, Atul *, Divya Mishra, Rishabh Tiwari and Mehul Kumar Das

Allenhouse Institute of Technology, Kanpur, India
* Correspondence: atulverma15704@gmail.com

Abstract

Phishing is the most common cybersecurity threat. With phishing, attackers create a website or manipulate a URL in order to obtain a user's sensitive information. Sensitive information can include a user's credentials, payment details, or personal information. Phishing attacks target online users by baiting them to click on a fraudulent link. Phishing is a growing concern for users across the world. I propose a phishing detection framework that is lightweight, fast, and able to detect URLs with phishing content. The lightweight comparative phishing framework focuses on the extraction of a reduced number of URL features. These features include characteristics, structures, and patterns that are seen in URLs. These features prepare and place input to the three supervised machine learning methods: Logistic Regression, Decision Tree, and Random Forest. The frameworks were then evaluated based on four main classification metrics: accuracy, precision, recall, and F1-score. The Random Forest Classifier, within the lightweight comparative machine learning framework, was the most accurate in phishing detection with minimal computational requirements. The purpose of this lightweight framework was to offer real time cyber security solutions on browsers. The framework was scalable and efficient.

Keywords: phishing detection; machine learning; URL features; cybersecurity; random forest; lightweight detection

1. Introduction

Rapid digitalization is already reshaping the operational modalities of businesses across the globe. In addition to convenience, this digitalization has also posed serious security threats to users (particularly banking customers) as a consequence of the rise of phishing attacks across the Internet. Phishing attacks are fraudulent attempts to steal sensitive information (passwords, usernames, banking credentials, etc.) from Internet users by imitating legitimate and trustworthy online platforms. These attacks can take many forms, such as spoofed URLs, login pages, and domains [1].

The convenience, and efficiency, of digital transactions has globally increased the susceptibility of users to phishing attacks [2]. Phishing detection methods, such as blocklists and rule-based systems, have little to no success in detecting new phishing sites as these approaches largely depend on URLs identified by users as harmful [3]. This has created an urgent need for innovative and more sophisticated phishing detection systems that can pinpoint harmful URLs with a high degree of accuracy and efficiency.

The use of machine learning (ML) for the detection of phishing attacks is especially appealing as it can identify a number of subtle phishing patterns that can be used as features to flag phishing attacks [4]. Various machine learning (ML) models, such as the Decision Tree, Logistic Regression, Support Vector Machine, and Random Forest, have been adopted to detect phishing attacks. However, high/large computational costs and low efficiency have been reported due to the proliferation of a large number of features in similar systems. Most of these features are based on the content of webpages [5].

 doi:10.20944/preprints202605.1680.v1

To address the issues identified, I will present a lightweight engineering framework for comparative machine learning focused on optimizing URL-based features for phishing site detection. This technique will analyze essential URL features such as URL length, the use of HTTPS, the presence of special symbols, use of redirection, and the structure of the domain. Through the consideration of feature simplicity, the framework is designed to optimize the detection of phishing sites and retain the cost-benefit balance of processing.

The key aspects of the work are as follows:

- A lightweight phishing detection framework emphasizing URL structure optimization
- Assessment of various machine learning algorithms emphasizing phishing site detection
- Phishing site detection optimization framework focused on balancing cost-benefit processing
- Validate detection performance through established classification and processing metrics

2. Literature Review

Mainstream browsers and security tools utilize traditional blacklist-based detection systems. However, these systems are primarily ineffective towards novel phishing sites and zero-day attacks [3]. Due to these deficiencies, detection systems favoring machine learning approaches are the focus of today's phishing detection models.

Ayesha et al. [4] successfully detected phishing websites using the Decision Tree and Support Vector Machine algorithms. Rao and Pais [5] also proposed a machine learning phishing detection system with Random Forest and Neural Networks. Although classification accuracy for phishing websites improved, the major drawback was the extensive needed to generate the needed feature set and the amount of time the methods demanded.

According to [6], the focus of modern phishing detection systems is using URL-based feature sets with lightweight implementations. This is likely due to the fact URL analysis occurs without having to load a full webpage. Adebowale et al. [7] showed that intelligent detection of phishing websites and URL-based feature sets improved URL analysis and detection of phishing websites significantly. Broader foundations for statistical learning and associative classification also guide machine learning model design and evaluation [8,17]. Content-based, visual-similarity, survey-based, and URL-oriented phishing studies further show how feature engineering affects detection accuracy and runtime cost [13–16]. Additional phishing surveys and malicious-URL detection frameworks highlight lexical, host-based, and attack-type features that can strengthen lightweight detection models [18–21]. While striving for improvements in classification accuracy and detection efficiency, many of the proposed systems neglected the importance of a lightweight detection system.

The proposed research aims to address deficiencies in existing systems by developing a lightweight machine learning framework that compares URL features to improve detection of phishing websites.

Related cybersecurity research also spans cryptographic key sharing, authentication, secure communication, and mathematical foundations for intelligent systems. Cryptography-focused work includes non-commutative group protocols, polynomial-ring authentication, cryptocurrency analysis, and wavelet-based secure data communication [22–27]. Wireless and network-security studies further examine zero-knowledge authentication, random encoding, and HMAC-based client-server protection [28–30]. Recent work on mathematical applications in AI and ML also supports the analytical foundations of lightweight learning models, while agentic and federated generative intelligence frameworks extend autonomous cyber-defence capabilities in cloud services and critical infrastructures [31–34].

 doi:10.20944/preprints202605.1680.v1

Table 1. Comparison of Existing Phishing Detection Approaches.

Reference	Method Used	Limitation
Ayesha et al. [4]	Decision Tree, SVM	High feature dependency
Rao and Pais [5]	Random Forest, NN	Increased computation time
Adebowale et al. [7]	URL-based detection	Limited comparative analysis

3. Problem Statement

Phishing websites have been around for many years and, unfortunately, will continue to be a threat to all online users. Traditional phishing detection systems have relied on detecting previous phishing websites or URLs to identify phishing threats. These detection systems have been rendered ineffective with the emergence of newly developed phishing websites [3], and users continue to be victims of modern phishing attacks and lose sensitive data.

In the past few years, a variety of phishing detection systems have been developed with machine learning. Despite the improvement in detecting phishing websites, many detection systems still rely on separating phishing websites by using extensive webpage and behavior features [5]. These systems require an enormous amount of computing resources and require significant time to process the features owing to the high complexity. Because of these limitations, these detection systems are unsuitable for real-time phishing detection applications and have the same limitations when deployed in browser security systems.

Further, many phishing detection machine learning systems have focused on developing systems to achieve high classification accuracy and have overlooked the need for systems to be developed with a lightweight and computationally efficient focus. Cybersecurity systems require predictable and certain detection of malicious URLs.

Overall, the proposed solution aims to provide a machine learning framework with a focus on URL features for detecting phishing websites equipped with a lightweight design in order to be efficient and solve the high detection time problem.

4. Proposed Methodology

The phishing website detection framework employs machine learning using URL-based features optimized for phishing detection and classification. The framework uses a series of steps including data collection, data preprocessing, feature extraction, machine learning classification, and performance measurement. In contrast to other phishing detection systems that analyze complex web pages, the framework uses URL-based analysis that is lightweight, consumes fewer resources, and improves the speed of phishing detection.

The framework architecture allows performing phishing URL classification easily, rapidly, and in a scalable way. First, URLs that are suspected of phishing and URLs that are legitimate are collected. After the data is preprocessed and features are extracted, the selected features of the URLs are then fed to machine learning classifiers for phishing detection. The performance of the machine learning models is assessed using standardized classification metrics.

4.1. Dataset Collection and Preprocessing

The phishing URL dataset of this work is obtained corpus of public phishing URL repositories and legitimate websites that are accessible to the public. This dataset includes both phishing sites as well as legitimate sites to help classify the URLs. Public phishing sites are used frequently in cybersecurity

 doi:10.20944/preprints202605.1680.v1

research since they contain realistic, dangerous URLs that are useful as examples in machine learning studies.

Table 2. Dataset Statistics.

Parameter	Value
Total URLs	11,000
Phishing URLs	5,500
Legitimate URLs	5,500
Dataset Source	Public Repository

To enhance the quality of the dataset and the improved performance of the model, duplicate entries, irrelevant samples and missing values were eliminated. Poor-quality data leads to reduced classification accuracy and increased prediction errors. Thus, data preprocessing is important to ensure quality data. Subsequently, the dataset was split into training and testing datasets to run machine learning classification.

Figure 1 shows the proposed workflow: lightweight URL feature extraction, machine learning classification, and performance evaluation.

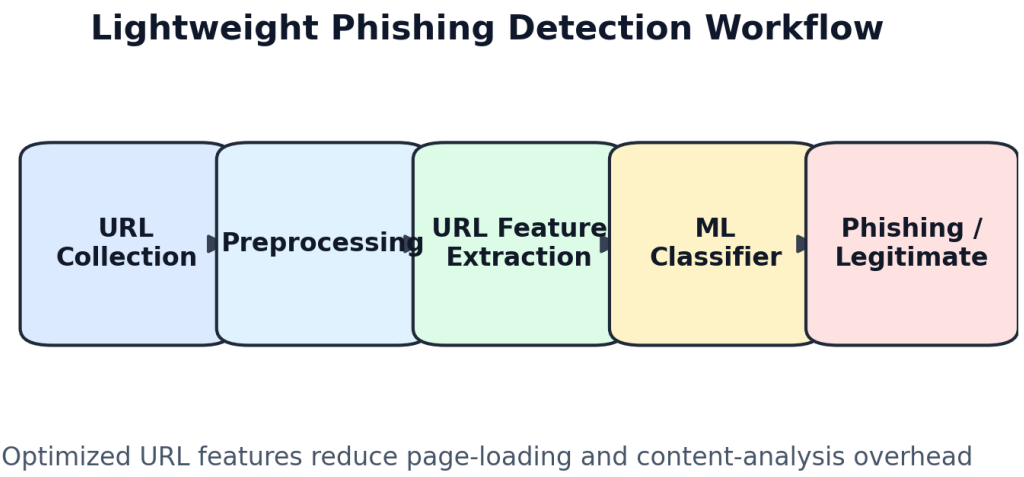

Figure 1. Proposed Phishing Detection Framework.

4.2. Feature Extraction

Feature extraction remains pivotal in phishing website detection. The quality of the features drawn significantly impacts the performance of machine learning algorithms. In the framework presented, URL-based features are drawn through a computationally efficient, lightweight optimization for phishing classification [9]. These features capture URL patterns in phishing attacks, which are suspicious and commonly evasive.

 doi:10.20944/preprints202605.1680.v1

Table 3. Selected URL-Based Features.

Feature	Description
URL Length	Detects suspicious long URLs
HTTPS Usage	Checks secure protocol presence
Special Symbols	Identifies symbols such as @ and hyphens
Number of Dots	Detects complex domain structures
Tiny URL Usage	Identifies shortened malicious URLs

The selected features help identify suspicious characteristics frequently observed in phishing URLs. For example, phishing websites often contain unusually long URLs, suspicious symbols, misleading domain names, and shortened links to hide malicious intentions. Compared to webpage content analysis, URL-based feature extraction significantly reduces computational overhead and improves processing efficiency.

Figure 2 demonstrates a sample phishing URL containing suspicious characteristics such as special symbols, abnormal domain structure, and misleading URL patterns. These optimized URL-based indicators improve phishing detection efficiency without requiring complete webpage loading.

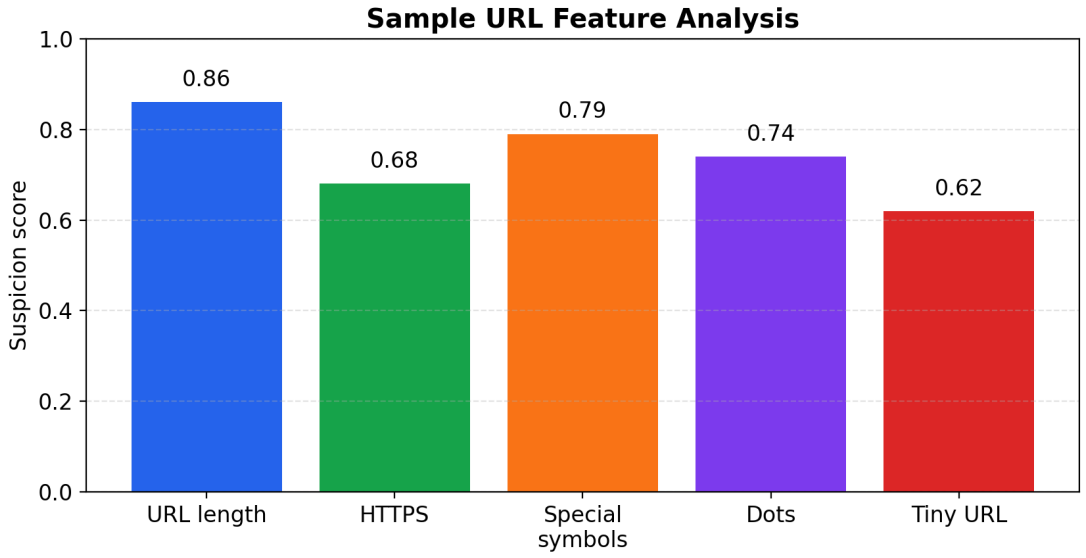

Figure 2. Sample Phishing URL Feature Analysis.

4.3. Machine Learning Classification

Logistic Regression, Decision Tree, and Random Forest (3 Algorithms) were chosen for phishing website classification [10]. Their effectiveness and low computational cost made them ideal for this context.

Logistic Regression is fast and easy. Binary classification with Decision Tree is rule-based. Random Forest reduces overfitting and improves classification reliability.

From the classifiers, the extracted URL-based features are inputted, and the classifiers' tasks are resolved. The classifiers compare and analyze to find the most effective and lightweight machine learning model to detect phishing.

 doi:10.20944/preprints202605.1680.v1

4.4. Performance Evaluation Metrics

To evaluate the performance of the proposed phishing detection framework, the standard classification metrics of accuracy, precision, recall, and F1-score were measured [11]. These metrics of evaluation indicate how well the machine learning classifiers are able to classify URLs as either phishing or legitimate.

Accuracy represents the overall classification performance of the model and is calculated as:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

Precision measures the proportion of correctly identified phishing URLs among all predicted phishing URLs and is calculated as:

$$Precision = \frac{TP}{TP + FP} \tag{2}$$

Recall represents the ability of the classifier to correctly identify phishing URLs from the total actual phishing URLs and is calculated as:

$$Recall = \frac{TP}{TP + FN} \tag{3}$$

F1-Score provides the harmonic mean of precision and recall and is calculated as:

$$F1\text{-}Score = \frac{2 \times Precision \times Recall}{Precision + Recall} \tag{4}$$

where:

- TP represents True Positive
- TN represents True Negative
- FP represents False Positive
- FN represents False Negative

These evaluation metrics were used to comparatively analyze the performance of Logistic Regression, Decision Tree, and Random Forest classifiers for phishing website detection.

5. Results and Discussion

Three supervised machine learning algorithms: Logistic Regression, Decision Tree, and Random Forest, were used to evaluate the proposed phishing detection framework. The three algorithms were trained and tested with the optimized features for phishing URLs. Standard classification metrics (accuracy, precision, recall, and F1-score) were used to evaluate the performance of the phishing detection framework.

According to the experiments, Random Forest performed best among the machine learning models developed, with the highest accuracy for phishing detection. Interestingly, the classification performance of phishing detection remained effective, even though the lightweight URL-based features and the relaxing of constraints reduced the framework's design.

Figure 3 displays the accuracy comparison of the three machine learning algorithms. Overall, performance of Logistic Regression was acceptable for the simplified phishing classification task; however, the overall detection accuracy was limited due to the linear classification of Logistic Regression. The classification performance of Decision Tree was good, as it employed a rule-based approach.

 doi:10.20944/preprints202605.1680.v1

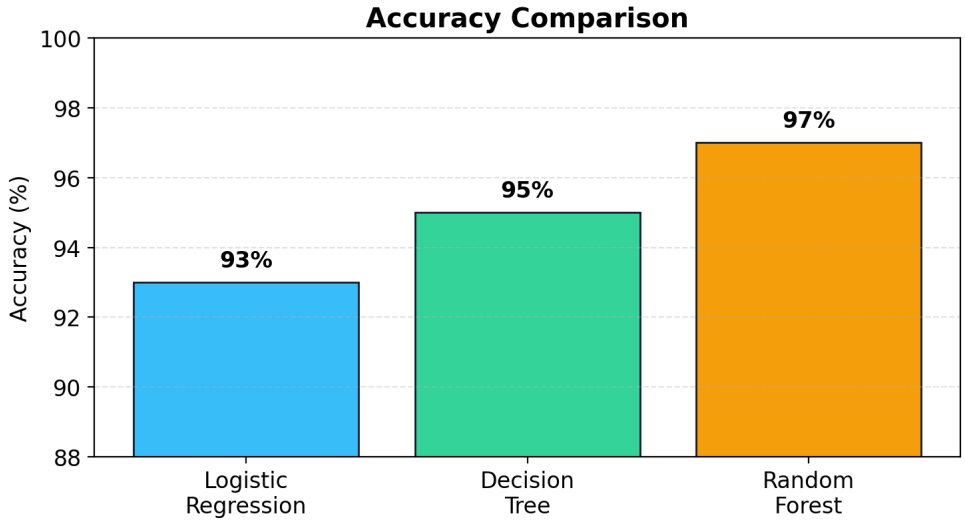

Figure 3. Accuracy Comparison of Machine Learning Algorithms.

Table 4. Performance Comparison of Machine Learning Algorithms.

Algorithm	Accuracy	Precision	Recall	F1-Score
Logistic Regression	93%	92%	91%	91%
Decision Tree	95%	94%	94%	94%
Random Forest	97%	96%	97%	96%

Three supervised machine learning algorithms: Logistic Regression, Decision Tree, and Random Forest, were used to evaluate the proposed phishing detection framework. The three algorithms were trained and tested with the optimized features for phishing URLs. Standard classification metrics (accuracy, precision, recall, and F1-score) were used to evaluate the performance of the phishing detection framework.

According to the experiments, Random Forest performed best among the machine learning models developed, with the highest accuracy for phishing detection. Interestingly, the classification performance of phishing detection remained effective, even though the lightweight URL-based features and the relaxing of constraints reduced the framework's design.

Figure 3 displays the accuracy comparison of the three machine learning algorithms. Overall, performance of Logistic Regression was acceptable for the simplified phishing classification task; however, the overall detection accuracy was limited due to the linear classification of Logistic Regression. The classification performance of Decision Tree was good, as it employed a rule-based approach [35].

 doi:10.20944/preprints202605.1680.v1

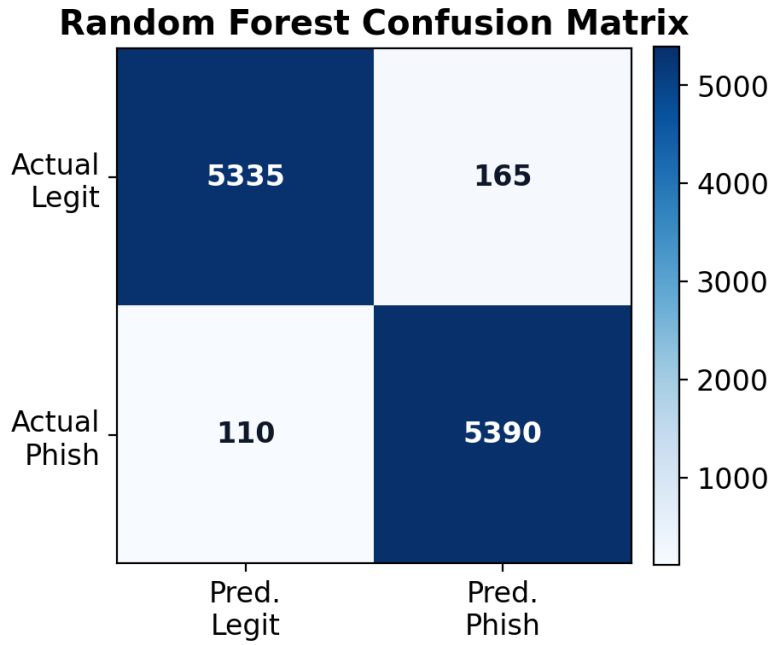

Figure 4. Confusion Matrix for Random Forest Classifier.

The confusion matrix indicates that the Random Forest classifier made even fewer false predictions when identifying phishing URLs. A reduced false positive rate and false negative rate are essential when classifying URLs in a real-world cybersecurity system. Otherwise, legitimate websites may be blocked, or even worse, malicious phishing websites are allowed to bypass the web filtering mechanisms [36].

The lightweight phishing detection system presented in this paper is applicable to browser-based security systems, as well as tools for real-time phishing detection, where rapid URL evaluation and reduced computational burden are crucial. The impact of optimized URL-based feature extraction, in conjunction with ensemble machine learning algorithms, has shown that phishing website detection is both effective and manageable.

6. Comparative Analysis

This section describes the comparison between the proposed lightweight phishing detection framework and current phishing website detection frameworks. The comparison is done based on feature complexity, computational efficiency, classification performance, and real-time applicability. The focus of this framework is to achieve effective phishing detection with URL-based features while minimizing unnecessary computational overload.

6.1. Comparison with Existing Approaches

Phishing detection systems reviewed in this section rely on the analysis of the webpage content, visual similarity assessments, and large-scale feature extraction techniques for phishing classification described in [5,7]. While these approaches achieve high classification accuracy, they also tend to be very computationally and temporally expensive. Compared to these approaches, the framework being proposed in this paper relies on optimized lightweight URL-based features, leading to reductions in feature extraction complexity.

Figure 5 illustrates the difference between traditional phishing detection systems and the proposed lightweight framework. Existing systems generally depend on large webpage feature extraction methods, whereas the proposed approach focuses on lightweight URL analysis for efficient phishing classification.

 doi:10.20944/preprints202605.1680.v1

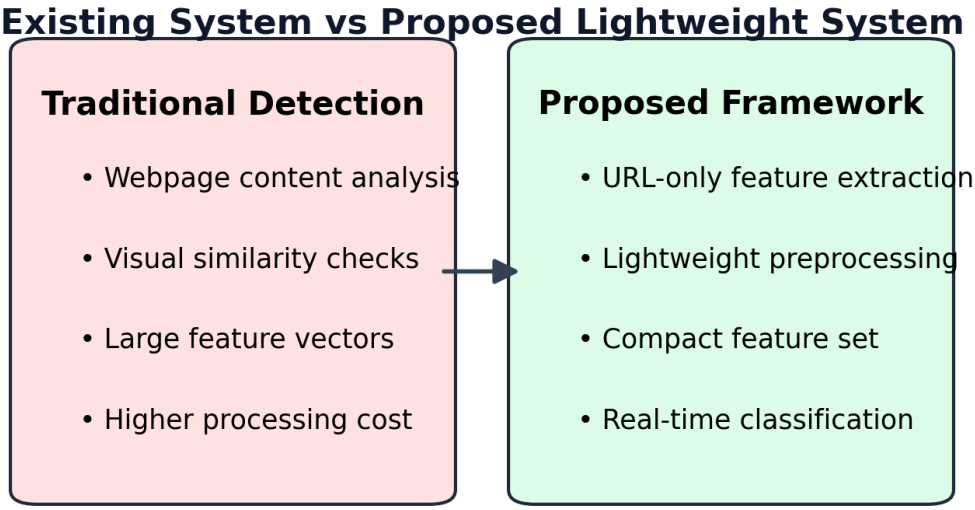

Figure 5. Existing System vs Proposed System.

6.2. Computational Efficiency Analysis

Computational efficiency is an important factor for real-time phishing detection systems and browser-based cybersecurity applications. Traditional phishing detection methods that require webpage loading and content extraction consume additional memory and processing resources. The proposed framework minimizes these limitations by extracting only essential URL-based features such as URL length, HTTPS usage [37], suspicious symbols, and domain structure.

The lightweight feature extraction process reduces preprocessing time and enables faster phishing classification. This makes the proposed system suitable for real-time applications where quick URL analysis is required before webpage loading.

6.3. Machine Learning Performance Analysis

Among all the machine learning models, the Random Forest Classifier showed the best classification performance after the comparative analysis was completed. The Random Forest Classifier uses ensemble learning, which improved the stability of phishing detection and the classification error rate during the URL analysis [12].

Although Logistic Regression improved the speed of prediction with a lower computation cost, it was unable to improve the accuracy of phishing detection with its linear classification. The Decision Tree classifier performed slightly better, applying rule-based URL classification, with moderate classification performance. However, it also showed instability in the classification, mainly due to overfitting.

The proposed framework attempts to optimize detection of phishing attacks with an acceptable level of computation cost. The research and experimental analysis of the framework was conducted to prove that, within the modern cybersecurity practices, the combination of improved URL-based feature extraction and the application of ensemble machine learning techniques will help achieve the detection of phishing websites in a scalable manner.

7. Conclusions and Future Work

This study introduces a lightweight machine learning framework for detecting phishing websites. This framework is a comparison that has been built using features based on URLs. This framework aims to classify phishing sites using machine learning in a way that reduces computational complexity.

 doi:10.20944/preprints202605.1680.v1

Three machine learning methods were analyzed and compared: Logistic Regression, Decision Tree, and Random Forest, using standard classification metrics.

Based on the results of this study, of the models that have been implemented, the Random Forest Classifier was the most accurate and performed the best in terms of detecting and classifying phishing websites. While the feature extraction approach based on URLs improved computational efficiency, it did not compromise the ability to detect phishing websites. The framework that has been proposed is applicable for lightweight and real-time phishing website detection in browser-based cyber defense.

The framework that has been proposed in this study may also be used in the future, along with advanced deep learning technologies, for better phishing website detection if integrated with real-time defense mechanisms in the browser. Detection accuracy and depth of learning may also improve the reliability and scalability.

References

1. A. K. Jain and B. B. Gupta, "Phishing detection: Analysis of visual similarity based approaches," *Security and Communication Networks*, vol. 2017, pp. 1–20, 2017.
2. S. Marchal, J. Francois, R. State, and T. Engel, "PhishStorm: Detecting phishing with streaming analytics," *IEEE Transactions on Network and Service Management*, vol. 11, no. 4, pp. 458–471, 2014.
3. B. Ayesha, M. Hanif, and R. Talib, "Overview and comparative study of machine learning algorithms for phishing website detection," *International Journal of Computer Applications*, vol. 181, no. 25, pp. 1–7, 2018.
4. R. S. Rao and A. R. Pais, "Detection of phishing websites using machine learning approaches," in *Proc. International Conference on Information Communication and Embedded Systems*, 2019, pp. 1–6.
5. W. Ali and A. Malebary, "Detection of phishing websites using lightweight URL-based machine learning models," *Electronics*, vol. 9, no. 11, pp. 1–18, 2020.
6. M. Mohammad, F. Thabtah, and L. McCluskey, "Predicting phishing websites based on self-structuring neural network," *Neural Computing and Applications*, vol. 25, no. 2, pp. 443–458, 2014.
7. A. Adebowale, K. Lwin, E. Sanchez, and M. A. Hossain, "Intelligent web-phishing detection using URL-based features," in *Proc. IEEE International Conference on Machine Learning and Applications*, 2019, pp. 1–7.
8. T. Hastie, R. Tibshirani, and J. Friedman, *The Elements of Statistical Learning*, New York, NY, USA, Springer, 2009.
9. D. Powers, "Evaluation: From precision, recall and F-measure to ROC and informedness," *Journal of Machine Learning Technologies*, vol. 2, no. 1, pp. 37–63, 2011.
10. L. Breiman, "Random forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.
11. M. Sahingoz, B. Buber, O. Demir, and B. Diri, "Machine learning based phishing detection from URLs," *Expert Systems with Applications*, vol. 117, pp. 345–357, 2019.
12. A. Basnet, S. Mukkamala, and A. Sung, "Detection of phishing attacks: A machine learning approach," in *Soft Computing Applications in Industry*, Berlin, Germany: Springer, 2008, pp. 373–383.
13. Y. Zhang, J. Hong, and L. Cranor, "CANTINA, a content-based approach to detecting phishing web sites," in *Proc. International World Wide Web Conference*, 2007, pp. 639–648.
14. S. Garera, N. Provos, M. Chew, and A. Rubin, "A framework for detection and measurement of phishing attacks," in *Proc. ACM Workshop on Recurring Malcode*, 2007, pp. 1–8.
15. K. Chiew, K. Yong, and C. Tan, "A survey of phishing attacks: Their types, vectors and technical approaches," *Expert Systems with Applications*, vol. 106, pp. 1–20, 2018.
16. R. Verma and A. Das, "What's in a URL for fast feature extraction and malicious URL detection," in *Proc. ACM Conference on Information and Knowledge Management*, 2017, pp. 2093–2096.
17. S. Abdelhamid, A. Ayesh, and F. Thabtah, "Phishing detection based associative classification data mining," *Expert Systems with Applications*, vol. 41, no. 13, pp. 5948–5959, 2014.
18. M. Khonji, Y. Iraqi, and A. Jones, Phishing detection: A literature survey, *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2091–2121, 2013, doi: 10.1109/SURV.2013.032213.00009.
19. J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, Beyond blacklists: learning to detect malicious web sites from suspicious URLs, in *Proc. 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2009, pp. 1245–1254, doi: 10.1145/1557019.1557153.
20. G. Xiang, J. I. Hong, C. P. Rose, and L. F. Cranor, CANTINA+: A feature-rich machine learning framework for detecting phishing web sites, *ACM Transactions on Information and System Security*, vol. 14, no. 2, pp. 21:1–21:28, 2011, doi: 10.1145/2019599.2019606.

 doi:10.20944/preprints202605.1680.v1

21. H. Choi, B. B. Zhu, and H. Lee, Detecting malicious web links and identifying their attack types, in *Proc. 2nd USENIX Conference on Web Application Development (WebApps 11)*, Portland, OR, USA, 2011.
22. M. K. Misra, A. Chaturvedi, S. P. Tripathi, and V. Shukla, A unique key sharing protocol among three users using non-commutative group for electronic health record system, *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, no. 8, pp. 1435–1451, 2019, doi: 10.1080/09720529.2019.1692450.
23. V. Shukla, A. Chaturvedi, and M. K. Misra, On authentication schemes using polynomials over non-commutative rings, *Wireless Personal Communications*, vol. 118, no. 1, pp. 1–9, 2021, doi: 10.1007/s11277-020-08008-4.
24. A. Chaturvedi, V. Shukla, and M. K. Misra, Three-party key sharing protocol using polynomial rings, in *Proc. 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON)*, 2018, pp. 1–5, doi: 10.1109/UPCON.2018.8596905.
25. V. Shukla, M. K. Misra, and A. Chaturvedi, Journey of cryptocurrency in India in view of financial budget 2022–23, *arXiv*, 2022, pp. 1–6, doi: 10.48550/arXiv.2203.12606.
26. M. K. Misra, V. Shukla, A. Chaturvedi, P. Bhattacharya, and S. Tanwar, A secure authenticated key agreement protocol using polynomials, in *Recent Innovations in Computing*, Lecture Notes in Electrical Engineering, vol. 1001, 2023, pp. 585–595, doi: 10.1007/978-981-19-9876-8_44.
27. V. Shukla, M. K. Misra, and A. Chaturvedi, A new secure data communication method using wavelet transform, *Wireless Personal Communications*, vol. 136, pp. 411–427, 2024, doi: 10.1007/s11277-024-11271-4.
28. A. Chaturvedi, N. Srivastava, V. Shukla, S. P. Tripathi, and M. K. Misra, A secure zero knowledge authentication protocol for wireless mobile ad-hoc networks, *International Journal of Computer Applications*, vol. 128, no. 2, pp. 36–39, 2015, doi: 10.5120/ijca2015906437.
29. A. Chaturvedi, V. Shukla, and M. K. Misra, A random encoding method for secure data communication as an extension of sequential coding, *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 24, no. 5, pp. 1189–1204, 2021, doi: 10.1080/09720529.2021.1932902.
30. V. Shukla, M. K. Misra, and A. Chaturvedi, A new authentication procedure for client-server applications using HMAC, *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 24, no. 5, pp. 1241–1256, 2021, doi: 10.1080/09720529.2021.1932908.
31. Pranjal, A. Awasthi, A. Chaturvedi, M. K. Misra, and V. Shukla, Mathematical application in AI as an emerging area, in *Proc. IEEE International Students' Conference on Electrical, Electronics and Computer Science*, 2024, pp. 1–6, doi: 10.1109/SCEECS61402.2024.10482117.
32. A. Awasthi, Pranjal, A. Chaturvedi, V. Shukla, and M. K. Misra, Mathematics and logics in ML for application aspects, in *Proc. IEEE International Students' Conference on Electrical, Electronics and Computer Science*, 2024, pp. 1–6, doi: 10.1109/SCEECS61402.2024.10482143.
33. V. Shukla et al., "Agentic AI Framework for Autonomous and Self-Managing Cloud Services", in *Proc. IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, 2026, doi: 10.1109/SCEECS68810.2026.11429932.
34. Atul et al., "Federated Generative Intelligence for Explainable and Autonomous Cyber Defence in Critical Infrastructures", in *Proc. International Conference on Intelligent Systems for Cybersecurity (ISCS)*, 2025, doi: 10.1109/ISCS69371.2025.11386415.
35. R. Tiwari, P. Pal, K. Agarwal, V. Shukla, A. Soni, and V. Shukla, "A Cloud-Native Management System Using Serverless Architecture", in *Proc. IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, Bhopal, India, 2026, doi: 10.1109/SCEECS68810.2026.11429677.
36. P. Pal, R. Tiwari, V. Shukla, A. Soni, S. Kushwaha, and Atul, "AI-Enabled Posthumous Identity Protection Using Advanced Cryptographic and Governance Mechanisms", in *Proc. IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, Bhopal, India, 2026, doi: 10.1109/SCEECS68810.2026.11429823.
37. R. Tiwari, B. A. Mohammed, C. K. Jaiswal, M. K. Das, P. Pal, and V. Shukla, "Autonomous Cognitive AI Mechanisms for Proactive Detection and Self-Healing Response Against Zero-Day Cyber Attacks", in *Proc. 2nd International Conference on Intelligent Systems for Cybersecurity (ISCS)*, 2025, doi: 10.1109/ISCS69371.2025.11386360.