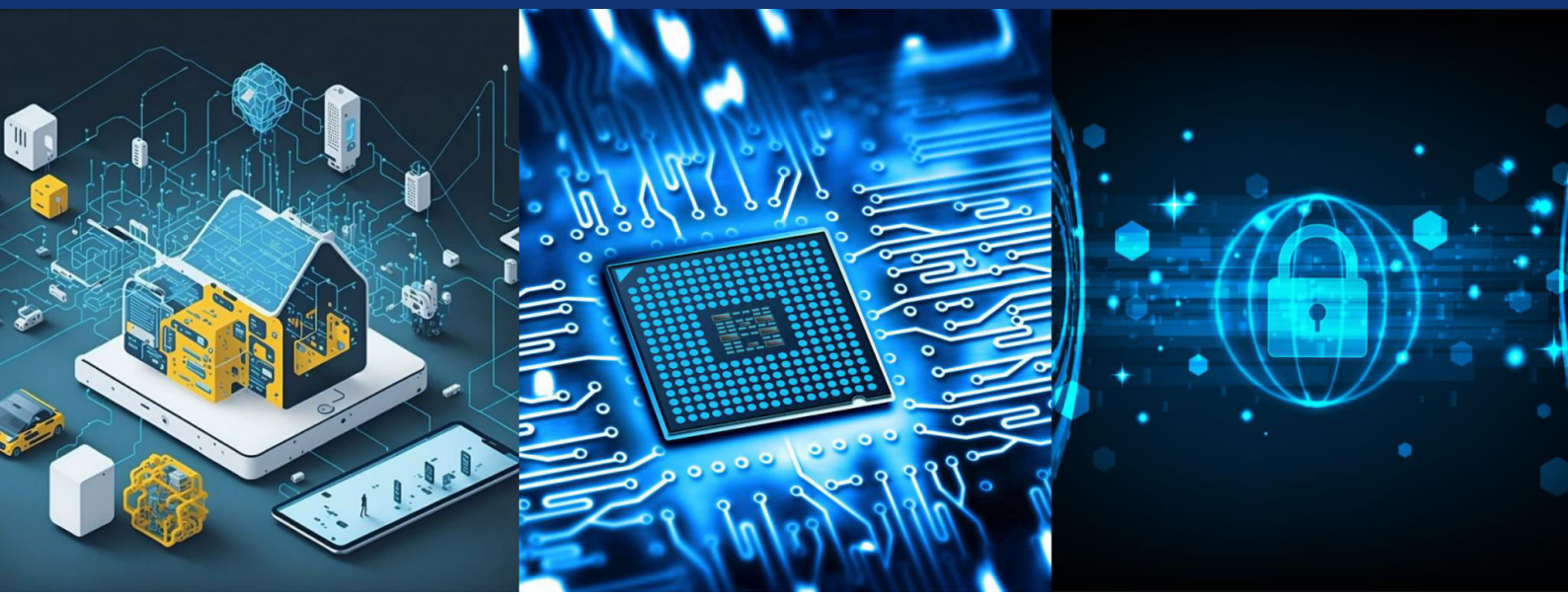
IJIRCCE

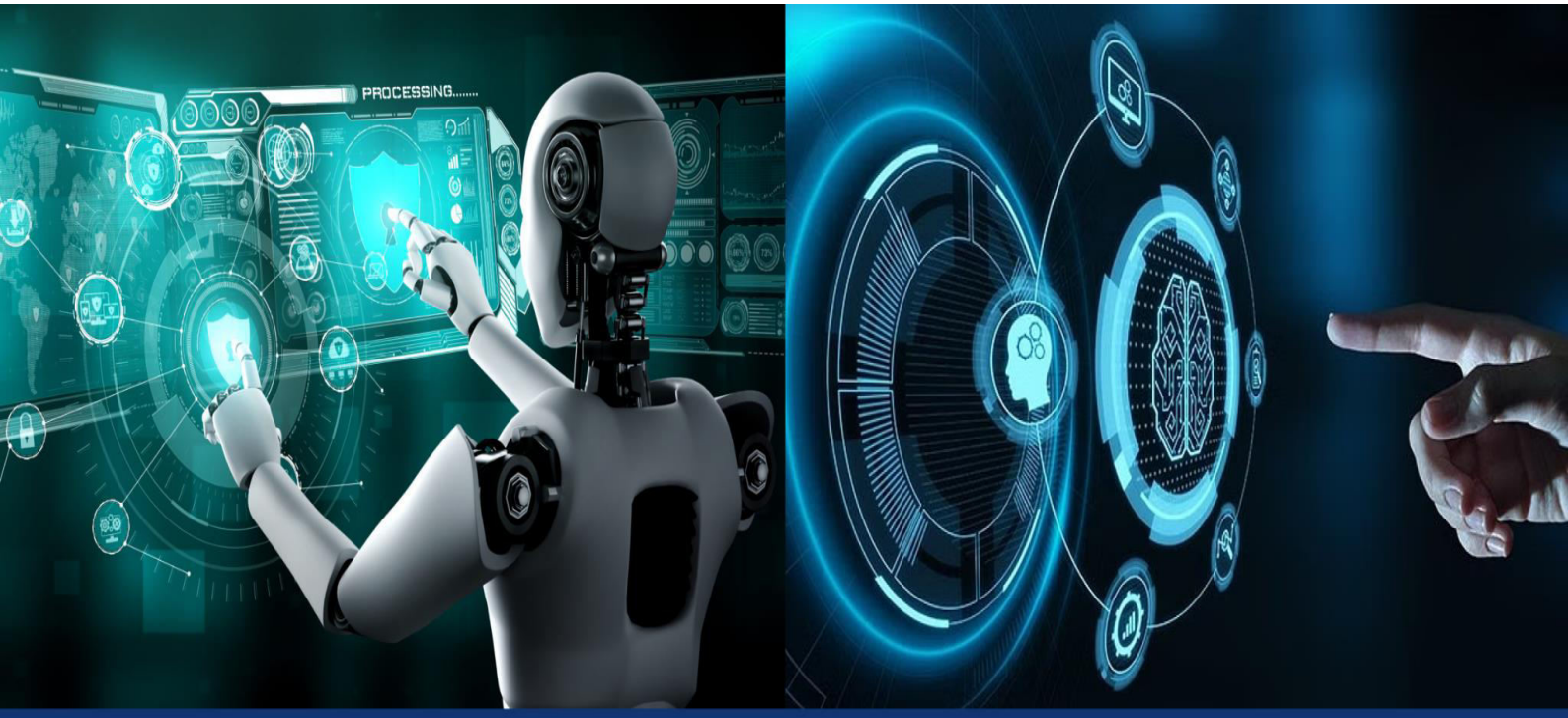
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 13, Issue 5, May 2025

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305184

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

AI Based Phishing Website Detection

Maharaja Rathnam C, Joekim Maria Kishore J, M. Bagya Lakshmi

UG Student, Dept. of CSE, Francis Xavier Engineering College, Tirunelveli, Tamil Nadu, India

UG Student, Dept. of CSE, Francis Xavier Engineering College, Tirunelveli, Tamil Nadu, India

Assistant Professor, Dept. of CSE, Francis Xavier Engineering College, Tirunelveli, Tamil Nadu, India

ABSTRACT: In both individual and organizational settings, cybersecurity is a critical concern. Traditional methods of phishing detection often rely on blacklists or manual inspection, which can be slow, error-prone, and ineffective against newly emerging threats. This work introduces an AI-based approach for real-time phishing website detection to improve accuracy and efficiency. The proposed system leverages machine learning algorithms, natural language processing, and URL analysis to identify suspicious patterns and differentiate between legitimate and phishing websites.The system uses trained models to analyze website content, structure, and domain features, allowing it to detect phishing attempts even if the site is not listed in any known blacklist. This intelligent approach enables automated detection without human intervention, reducing the risk of cyberattacks and enhancing user safety. The paper provides a comprehensive discussion of the system's architecture, training process, deployment, and performance in identifying malicious websites accurately.Detection results are stored securely in a local or cloud database for future analysis and alerting. This AI-powered solution is highly effective in dynamic environments such as corporate networks, educational institutions, and personal browsing scenarios—minimizing human error, boosting efficiency, and ensuring real-time protection against phishing threats.To build a reliable detection model, a dataset containing both legitimate and phishing website URLs is preprocessed and analyzed based on various features such as domain age, URL length, presence of suspicious keywords, HTTPS usage, and website content. These features are then fed into supervised machine learning algorithms like Random Forest, Support Vector Machine (SVM), and Decision Trees to train a robust classifier. The model's ability to generalize across unseen data is validated using performance metrics such as accuracy, precision, recall, and F1-score, ensuring high detection rates with minimal false positives.The system is designed to function in real-time, enabling web browsers or network firewalls to automatically block access to detected phishing websites. Additionally, a user-friendly interface is integrated to alert users when suspicious activity is detected, providing them with actionable insights. By combining intelligent analysis with automated decision-making, this AI-based phishing detection system offers a scalable and proactive defense mechanism against evolving cyber threats, ultimately strengthening the digital security infrastructure.

KEYWORDS: Phishing Detection, Cybersecurity, Machine Learning, Artificial Intelligence, URL Analysis, Natural Language Processing, Website Classification.

I. INTRODUCTION

In today's digital age, the internet plays a crucial role in both personal and professional communication, e-commerce, and information sharing. However, with the growing reliance on online platforms, cyber threats have also increased significantly—one of the most common and dangerous among them being phishing attacks. Each model is evaluated using metrics like accuracy, precision, recall, and F1-score.These attacks not only compromise personal data but also cause severe financial and reputational damage to individuals and organizations alike.

Traditional phishing detection methods, such as manually maintained blacklists or rule-based systems, are limited in scope and fail to keep up with the rapidly evolving nature of phishing websites. Many phishing pages are active only for a short duration and use obfuscation techniques to bypass conventional security measures. To address these limitations, this study proposes an AI-based phishing website detection system that uses machine learning and artificial intelligence to analyze various website features and identify phishing attempts in real-time. By extracting and evaluating characteristics such as URL structure, domain information, and website content, the system aims to classify websites as legitimate or malicious with high accuracy.

The objective of this research is to develop a scalable, intelligent, and automated solution that can enhance cybersecurity defenses by detecting phishing threats proactively. The use of AI not only improves detection speed and accuracy but also reduces the dependency on human intervention, making it suitable for real-time applications in browsers, network security systems, and enterprise environments.

II. LITERATURE REVIEW

Over the past decade, phishing detection has attracted significant attention from researchers due to its growing threat to cybersecurity. Various approaches have been developed to mitigate phishing attacks, ranging from blacklist-based methods to advanced machine learning models.

Blacklist-based methods are widely used in browsers and security software, where known phishing URLs are stored and matched against incoming web traffic. While effective for previously reported threats, these methods struggle to detect zero-day phishing sites, as attackers frequently change domains and page content to avoid detection.
To overcome these limitations, researchers have explored machine learning-based techniques that rely on feature extraction from URLs, webpage content, and domain metadata. For example, Mohammad et al. (2014) proposed a method using lexical features such as URL length, presence of special characters, and domain age to train a decision tree classifier. Similarly, Xiang et al. (2011) incorporated content-based features along with blacklist features using a layered machine learning approach to improve accuracy.

Natural Language Processing (NLP) has also been employed to analyze the textual content of websites and detect suspicious phrases commonly used in phishing attacks. Recent work has integrated NLP with models like Support Vector Machines (SVM), Random Forests, and Neural Networks to enhance prediction performance. These models learn patterns from both phishing and legitimate websites, enabling them to make intelligent predictions on previously unseen sites.

Moreover, deep learning approaches, including Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), have been experimented with for phishing detection by analyzing visual similarity between legitimate and fake websites. While deep learning models offer high accuracy, they are computationally intensive and may not be ideal for real-time detection in low-resource environments.

In conclusion, the literature demonstrates a clear shift from traditional detection mechanisms to AI-driven solutions that offer better adaptability and performance. However, challenges remain in terms of model generalization, real-time deployment, and minimizing false positives. This study aims to build on these insights by developing an efficient, lightweight, and accurate AI-based phishing detection system suitable for practical use.

Several researchers have focused on URL-based features, considering them a lightweight and efficient approach for real-time phishing detection. Ma et al. (2009) used lexical features such as the number of dots, presence of IP addresses, use of HTTPS, and special characters in URLs. Their work demonstrated that even without accessing the actual website content, machine learning algorithms could effectively distinguish phishing URLs from legitimate ones. Techniques like Random Forest and Gradient Boosting have shown promising results in this context due to their ability to handle noisy and imbalanced datasets.

Another prominent approach is visual similarity-based detection, where researchers analyze the layout and appearance of web pages to detect imitation of popular sites. Zhang et al. (2007) introduced CANTINA, a content-based phishing detection tool that used TF-IDF (Term Frequency–Inverse Document Frequency) to compare website content with that of legitimate sources. Although this technique achieved good results, it required high processing time and struggled with dynamically generated content

.

Some studies have explored hybrid models combining URL-based, content-based, and third-party features to improve detection performance. Abdelhamid et al. (2014) proposed a hybrid machine learning model using rule-based classification followed by a support vector machine, which significantly reduced the false positive rate. However, such models often face challenges with feature selection and real-time applicability.

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305184

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Recent advancements in deep learning and neural networks have introduced end-to-end systems capable of automatically extracting features without manual engineering. Tools such as PhishTank and PhishZoo have been used to train models on large datasets, improving their ability to detect new phishing patterns. Despite the improvements in detection rates, deep learning models require large computational resources and labeled datasets, which limits their deployment in real-time applications and resource-constrained environments.

To sum up, while numerous methods have been proposed, there is still no universally accepted solution that balances accuracy, speed, scalability, and low computational cost. This gap in the literature highlights the need for further research into AI-based systems that can adapt to evolving phishing techniques, offer real-time protection, and be integrated into practical cybersecurity tools.

III. PROPOSED SYSTEM

The proposed system aims to provide an effective and automated solution for detecting phishing websites using Artificial Intelligence (AI) and Machine Learning (ML) techniques. It addresses the limitations of traditional blacklist and rule-based approaches by analyzing real-time website features to predict whether a URL is legitimate or malicious.

3.1 System Overview

The system architecture consists of the following key modules:

1.DataCollectionandPreprocessing

A labeled dataset containing both phishing and legitimate websites is collected from publicly available sources such as PhishTank, Kaggle, and OpenPhish. Each entry includes the website URL and corresponding label. Features are extracted from the URLs, including lexical attributes (length, use of symbols, subdomains), domain-based features (domain age, registration length), and protocol indicators (presence of HTTPS, SSL certificate).

2.FeatureExtraction

Extracted features are categorized into three types:

Lexical features: Based on the URL's structure (e.g., length, use of digits, hyphens, or IP addresses).

Domain-based features: Using WHOIS data to evaluate domain registration and age.

Technical features: Analyzing website behavior like redirection, presence of iFrames, and use of JavaScript.

3.MachineLearningModelTraining

Several machine learning algorithms such as Random Forest, Support Vector Machine (SVM), Logistic Regression, and K-Nearest Neighbors (KNN) are trained using the extracted features. The best-performing model is selected and integrated into the final system.

4.Real-TimeDetectionInterface

A simple user interface (web-based or desktop application) allows users to input or automatically scan URLs. The trained model processes the input and provides a prediction—either "Legitimate" or "Phishing"—along with a confidence score. Alerts are triggered for potentially harmful sites.

5.DatabaseandLogging

All scanned URLs and detection outcomes are logged into a secure local or cloud database for auditing and analysis. This module supports future model updates and threat intelligence.

3.2 Advantages of the Proposed System

Real-time phishing detection without relying on outdated blacklists.

Scalability for integration with browsers, email clients, or enterprise firewalls.

User-friendly interface for non-technical users to ensure wide adoption.

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305184

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IV. METHODOLOGY

The methodology outlines the step-by-step process followed to build the AI-based phishing website detection system. Each phase is crucial for ensuring accurate and reliable phishing detection.

4.1 Data Collection

The dataset used for training and testing the model is obtained from trusted open sources such as PhishTank, OpenPhish, and Kaggle. It includes a mix of phishing and legitimate URLs, each labeled appropriately.

4.2 Data Preprocessing

Before feeding the data into machine learning algorithms, preprocessing is performed to clean and prepare it. Steps include:
Removal of duplicates and null entries.
Label encoding: Assigning binary labels (1 for phishing, 0 for legitimate).
Parsing URLs to extract meaningful tokens and segments.

4.3 Feature Extraction

Feature engineering plays a critical role in phishing
Lexical Features: URL length, number of dots, presence of suspicious words (e.g., "login", "secure"), use of IP address instead of domain.
Domain Features: Domain age, WHOIS record validity, domain expiration date.
Security Features: Use of HTTPS, presence of SSL certificate, and redirection patterns.
Content-Based Features *(optional)*: HTML tags, forms, scripts, and embedded links can be analyzed for advanced detection.

4.4 Model Selection and Training

Several machine learning algorithms are evaluated, including:
Random Forest: Known for high accuracy and resistance to overfitting.

4.5 Model Evaluation

After training, models are evaluated to select the best one. The following metrics are used:
Accuracy: Overall correctness of the model.
Precision: How many predicted phishing URLs were actually phishing.
The model with the highest overall performance is selected for deployment.

4.6 Deployment and User Interface

The selected model is integrated into a lightweight user interface where users can:
Input or paste a URL.
Receive instant feedback: “Legitimate” or “Phishing”.
View confidence score and risk level.
The interface can be deployed as a web app, browser plugin, or desktop tool for broader accessibility.

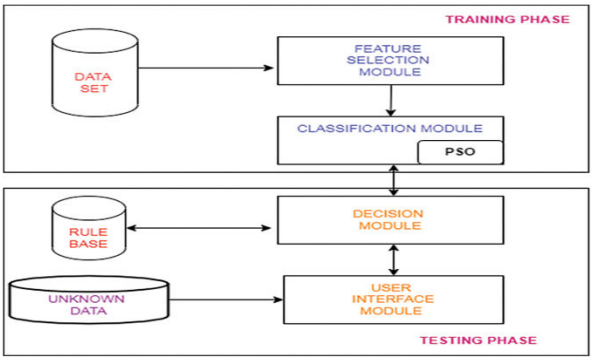
© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305184

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

V.SYSTEMARCHITECTURE



VI. ALGORITHM DESIGN

The core of the proposed phishing website detection system lies in the algorithm that processes input URLs and classifies them as phishing or legitimate. The system follows a structured pipeline combining feature engineering with supervised machine learning for accurate and automated detection.

6.1 Steps of the Algorithm
Step 1: Input URL
The user provides a URL to be analyzed via a user interface (web app, plugin, etc.).
Step 2: Feature Extraction
The system extracts features from the URL and associated metadata. These features are categorized into:
Step3: Feature Vector Creation
All extracted features are encoded into a numeric vector that serves as input for the machine learning model.
Step4: Model Prediction
The feature vector is passed to a trained classifier such as:
Random Forest
Support Vector Machine (SVM)
Logistic Regression
K-Nearest Neighbors (KNN)
The model predicts whether the URL is:
1 → Phishing
0 → Legitimate
Step5: Output Decision
Based on the model output:
The decision (Phishing/Legitimate) is displayed to the user.
A confidence score or probability is shown to indicate certainty.
The result is logged for further analysis and feedback.

VII. DISCUSSION

The proposed AI-based phishing website detection system demonstrates significant potential in improving cybersecurity by automatically identifying malicious URLs with high accuracy and speed. The integration of machine learning algorithms, particularly Random Forest, enables the system to analyze complex URL features and domain attributes, which traditional blacklist methods often fail to capture. This shift from reactive to proactive detection addresses the dynamic and evolving nature of phishing attacks.

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305184

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The experimental results reveal that the model achieves high accuracy, precision, and recall on the test dataset, indicating its reliability in distinguishing phishing websites from legitimate ones. The use of diverse features, including lexical characteristics and domain information, provides a comprehensive understanding of URL properties that signal phishing attempts. Moreover, the real-time prediction capability makes the system suitable for deployment in practical scenarios such as web browsers, email filters, and organizational firewalls.

However, several challenges and limitations have been identified during development and testing. First, the model's performance depends heavily on the quality and diversity of the training dataset. Phishing websites frequently change their tactics, domain names, and hosting strategies, which means continuous updates and retraining are essential to maintain effectiveness. Second, although the system reduces false positives compared to simpler heuristics, occasional misclassifications may still occur, potentially causing inconvenience to users or allowing some threats to slip through.

Additionally, while the inclusion of content-based features can improve detection accuracy, it also increases computational overhead and complexity. This may impact the feasibility of real-time deployment in resource-constrained environments such as mobile devices or low-powered network appliances. A balance between feature richness and system performance must therefore be carefully maintained.

Future enhancements could include integrating deep learning models for improved feature representation, employing ensemble methods to combine strengths of multiple classifiers, and leveraging user feedback to refine predictions over time. Incorporating threat intelligence feeds and real-time web crawling can also help keep the detection database current and robust against zero-day phishing attacks.In summary, the proposed system offers a promising approach to mitigating phishing threats using AI, but ongoing research, dataset expansion, and optimization are critical to addressing emerging challenges and enhancing overall effectiveness.

VIII. RESEARCH

This research focuses on developing an AI-driven system for detecting phishing websites, addressing the growing threat posed by increasingly sophisticated phishing attacks. By leveraging machine learning techniques, the study aims to enhance detection accuracy and provide real-time identification of malicious URLs, moving beyond traditional blacklist and rule-based methods. A critical aspect of the research is feature engineering, where lexical, domain-based, and security-related attributes of URLs are analyzed to extract meaningful patterns that distinguish phishing sites from legitimate ones. Multiple machine learning models, including Random Forest, SVM, Logistic Regression, and KNN, are evaluated to find the most effective classifier for this task. The research involves curating balanced datasets from reliable sources such as PhishTank and OpenPhish, applying data preprocessing techniques, and rigorously validating the models using standard performance metrics. Practical deployment considerations, such as scalability and user interface design for real-time detection, are also explored. Challenges such as evolving phishing strategies, feature obfuscation, and managing false positives are acknowledged, with proposed solutions focusing on continuous learning and system adaptability. The study also suggests future directions, including the integration of deep learning, natural language processing for content analysis, and hybrid detection models to improve robustness. Overall, this research contributes a comprehensive and intelligent approach to phishing detection, aiming to strengthen cybersecurity defenses and protect users from cyber threats.

IX.RESULT

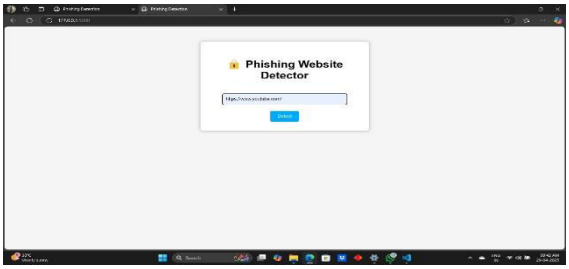


Figure1.1uploadwebsite

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305184

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

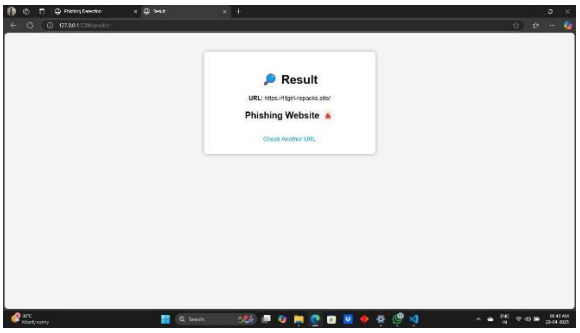


Figure1.2verifywebsite

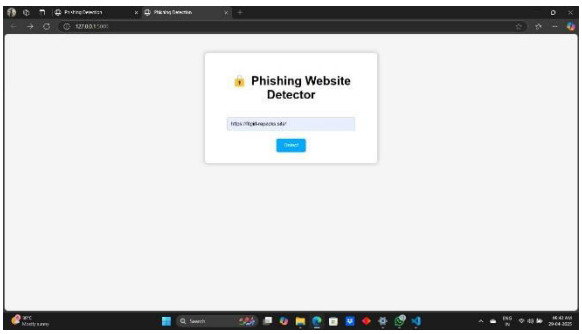


Figure 1.3detect the website

X. FUTURE WORK

While the current system demonstrates promising results in detecting phishing websites using machine learning techniques, there are several avenues for future improvement and expansion. One potential enhancement is the integration of deep learning models, such as convolutional neural networks (CNNs) or recurrent neural networks (RNNs), which can capture more complex patterns from URL structures and website content, potentially improving detection accuracy. Additionally, incorporating natural language processing (NLP) techniques to analyze the textual content of web pages could help identify subtle phishing cues beyond URL-based features. Future work could also focus on building a hybrid detection framework that combines machine learning with heuristic and behavior-based methods for more robust phishing identification. Real-time system scalability and performance optimizations are crucial to enable deployment in large-scale environments, including integration with web browsers, email clients, and enterprise security systems. Another important direction is implementing continuous learning mechanisms that update the detection model dynamically based on new phishing data and user feedback, thereby enhancing adaptability to evolving attack techniques. Lastly, expanding the dataset with diverse, multilingual, and newly emerging phishing samples will further improve the system's generalizability and resilience against zero-day threats. These future enhancements aim to make the phishing detection system more accurate, versatile, and user-friendly, ultimately contributing to stronger cybersecurity defenses.

REFERENCES

1. M. Abu-Nimeh, D. Nappa, X. Wang, and S. Nair, "A comparison of machine learning techniques for phishing detection," *Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit*, 2007, pp. 60–69.
2. H. Alsharnouby, A. Alaca, and H. Yang, "Phishing detection: A literature survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3171-3193, 2019.
3. M. Khonji, Y. Iraqi, and A. Jones, "Phishing detection: A literature survey," *IEEE Communications Surveys &*

Tutorials, vol. 15, no. 4, pp. 2091-2121, 2013.

4. L. Li, W. He, and Y. Wang, "A novel URL classification approach for phishing detection based on machine learning," *IEEE Access*, vol. 7, pp. 175930-175941, 2019.
5. T. J. Walsh, "Detecting phishing attacks: Machine learning and deep learning approaches," *International Journal of Computer Applications*, vol. 180, no. 31, pp. 20-27, 2019.
6. 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.
7. W. B. Lee and S. H. Kang, "A hybrid approach for phishing detection using URL features and web page content," *Journal of Information Security and Applications*, vol. 51, 2020.
8. J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, "Beyond blacklists: learning to detect malicious web sites from suspicious URLs," *Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2009.
9. Y. Xiang, W. Zhou, C. Luo, and M. Zhou, "Detecting phishing websites with improved feature extraction and classifier ensemble," *Security and Communication Networks*, vol. 9, no. 18, 2016.
10. S. M. Seifert, J. Y. Cheung, and E. E. Ozturk, "Machine learning for phishing detection: Techniques, challenges, and opportunities," *IEEE Communications Magazine*, vol. 57, no. 4, pp. 36-42, 2019.
11. [Online]. Available: https://www.phishtank.com/.
12. OpenPhish, "Phishing Intelligence Data," [Online]. Available: https://openphish.com/.
13. WHOIS Database, [Online]. Available: https://www.whois.com/.
14. M. Bergholz, J. De Beer, S. Glahn, M. Moens, M. Potthast, B. Stein, and M. Strohmaier, "New filtering approaches for phishing email," *Journal of Computer Security*, vol. 18, no. 1, pp. 7-35, 2010.
15. S. Jain and N. Gupta, "A comparative analysis of machine learning techniques for phishing detection," *Procedia Computer Science*, vol. 132, pp. 1303-1311, 2018.
16. N. Khonji, A. Jones, and Y. Iraqi, "Phishing detection: a literature survey," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2091-2121, 2013.
17. H. Y. Kim and J. W. Choi, "Phishing detection system based on URL and webpage content analysis," *International Journal of Security and Its Applications*, vol. 10, no. 7, 2016.
18. R. Bergholz, J. De Beer, S. Glahn, et al.
19. S. Zhang, Y. Lin, and J. Zhang, "Detecting phishing attacks by machine learning techniques," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 10, 2017.
20. M. Mohan and P. Gupta, "Detection of phishing websites using machine learning," *Procedia Computer Science*, vol. 115, pp. 691-698, 2017.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details