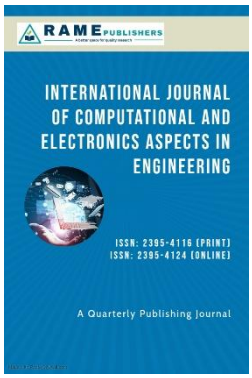
International Journal of Computational and Electronic Aspects in Engineering
Volume 7, Issue 3, July 2026, pp 15-21
Special Issue of National Conference on Emerging Innovative Trends in Computer Applications
https://doi.org/10.26706/ijceae.7.3.20260703

PhishGuard: A Real-Time Email and Web Phishing Detector

Rupesh Bangre*, Mehul Mishra, Harshika Likhar, Sakshi Samrutwar

MCA Department, Saryodaya College of Engineering and Technology, Nagpur, India

Corresponding Author: rupesh.rpb@gmail.com



Abstract: Phishing attacks have become one of the most common and dangerous cyber threats in the modern digital era. Attackers exploit human trust through deceptive emails and fraudulent websites to steal sensitive information such as login credentials, financial data, and personal details. Traditional phishing detection mechanisms, such as blacklist-based filtering and rule-based systems, are often ineffective against newly generated and zero-day phishing attacks.This paper introduces PhishGuard, a real-time phishing detection system that uses Artificial Intelligence (AI), including machine learning and natural language processing, to identify suspicious emails and web links.PhishGuard focuses on user-side protection by providing instant risk analysis and understandable alerts. The system aims to improve dete5ction accuracy, reduce false positives, and enhance cybersecurity awareness among users.

Keywords: phishguard, zero-day phishing , machine learning, cybersecurity ,phishing detector.

1.

Article – Peer Reviewed
Received: 1 March 2026
Accepted: 30 June 2026
Published: 31 July 2026

Cite this article: Rupesh Bangre, Mehul Mishra, Harshika Likhar, Sakshi Samrutwar, "PhishGuard: A Real-Time Email and Web Phishing Detector", *International Journal of Computational and Electronic Aspects in Engineering*, vol. 7, issue 3, pp. 15-21, 2026. https://doi.org/10.26706/ijceae.7.3.20260703

1. Introduction

As internet usage has grown rapidly, communication through emails and websites has become a regular part of everyday life. However, this growth has also increased cybercrime, especially phishing attacks. Phishing is a type of social engineering attack where attackers pretend to be trusted organizations to trick users into sharing confidential information. According to cybersecurity reports, phishing continues to be the main cause of data breaches across different industries. Most existing solutions depend on fixed rules, known phishing databases, or advanced security tools that are not easily available to individual users. These methods often fail to detect new phishing messages that are designed to bypass traditional filters. This creates a necessity for a quick, easy and real - time phishing detection system. PhishGuard is designed to solve this problem by analyzing emails and URLs in real time and warning users before any harm can happen.

Many current methods rely on rule-based techniques, known phishing datasets, or large-scale security systems that are not easily accessible to individual users. As a result, these methods may struggle to detect newly emerging phishing attacks detecting new phishing messages that manage to get past traditional filtering systems. [7]. This creates a necessity for a simple, fast, and real-time phishing detection system. PhishGuard is designed to solve this problem by analyzing emails and URLs in real time and warning users before any harm can happen.

2. Literature Reviews

2.1 Effectiveness and Efficiency of PhishGuard

PhishGuard enhances detection by analyzing data in real time instead of depending only on existing phishing databases. It evaluates email content, URLs, and patterns

immediately after they are received, which enables early identification of potential phishing attempts.to detect new phishing attempts that may not be identified by traditional filters.[7] It uses Artificial Intelligence (AI), including machine learning and natural language processing, to continuously improve its detection by learning from new data.In terms of efficiency, the system is designed to process inputs quickly with minimal computational overhead, making it suitable for everyday use without affecting system performance. Its lightweight architecture ensures fast response times while providing clear and understandable alerts to users, helping them make informed decisions without technical complexity.[2]

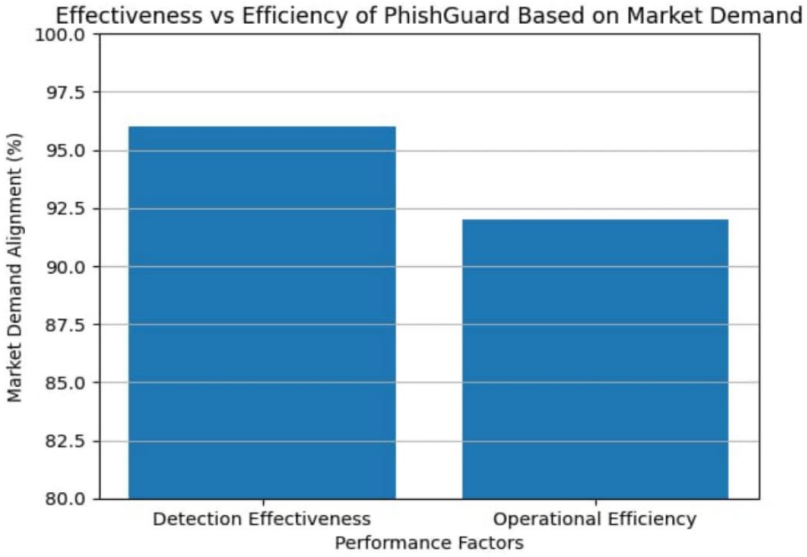


Figure 1. Effectiveness vs Efficiency of Phishgaurd Based on Market Demand

2.2 Methodology

1. Machine Learning-Based Phishing Detection
Researchers have developed systems that use Artificial Intelligence (AI), especially machine learning models like Decision Trees and Naive Bayes, to classify URLs as either phishing or safe. These systems have achieved accuracy of around 95.4% on large datasets, showing that such models can effectively identify malicious websites based only on URL features [11].

2. Comparison of Multiple Machine Learning Models
Another study compared different Artificial Intelligence (AI) models, including machine learning techniques such as Random Forest, SVM, Neural Networks, and Logistic Regression, for detecting phishing websites. The results showed that combining these models can increase accuracy to over 97%, and they can also be used in real-world web applications to check links effectively [11].

3. Use of Ensemble and Deep Learning Models for Phishing Detection
Some recent studies have used deep learning approaches by combining models like LSTM and XGBoost. These models analyze the URL text directly and identify patterns on their own, without needing manually selected features. In some experiments, these methods achieved accuracy of about 96%. This suggests that deep learning models are more effective in handling new and changing phishing techniques [12].

4. Using CNN-Based Deep Learning for Phishing Detection
Some studies have applied convolutional neural networks (CNNs) to analyze website content and structure for detecting phishing websites. These approaches have reported detection rates of more than 98% and perform better than many traditional machine learning methods. This shows that deep learning techniques can be very useful for solving phishing detection problems [8].

5. Recent Developments in Machine Learning for Phishing Detection
In a study conducted in 2024, researchers used Random Forest models trained on real phishing datasets and achieved accuracy of up to 99.4%. The system was also deployed as a browser extension to provide real-time detection. This indicates that machine learning models can not only achieve high accuracy but also be practical for real-world use [7].

2.3 Qualitative and Quantitative Analysis

2.3.1 Qualitative and Quantitative Evaluation of Phishing Detection Techniques

Over the past decade, phishing detection techniques have improved in terms of both performance and overall effectiveness. Several studies have shown that supervised machine learning models like Random Forest and CNNs perform well in detecting phishing attacks. In many cases, these models have achieved accuracy above 97%. This indicates that they perform reliably when tested on standard datasets. For example, CNN-based approaches have reported detection rates as high as 98.2%, along with strong F1-scores in identifying phishing and legitimate websites. These results are generally better than those of traditional machine learning methods tested on the same data. [11]

2.3.2 Significance of Qualitative and Quantitative Performance Metrics in Phishing Detection

1. Evaluation of Detection Accuracy Metrics

In this study, performance is mainly evaluated based on how accurately the system can classify phishing and legitimate emails or URLs. Traditional machine learning models usually provide moderate accuracy because they depend on manually selected features and do not adapt well to new phishing patterns. Deep learning models can improve detection by automatically learning patterns from data, but they often need large datasets and more computational power.

PhishGuard performs better because it uses multiple types of features, such as URL structure, email content, and user behavior. By analyzing both data patterns and context, the system is able to reduce false positives and false negatives, which improves its overall accuracy. In addition, the system can update itself using recent phishing data, which helps it detect new types of attacks more effectively than older static models.[10]

2. Evaluation of Qualitative Performance (Efficiency and Practical Use)

The qualitative evaluation focuses on how efficient the system is and how well it works in real-world situations, not just on numerical results. It takes into account factors like response time, scalability, ease of use, ability to handle new types of attacks, and how easy it is for users to understand the results. Earlier phishing detection systems provided acceptable accuracy, but many of them were slow, required frequent manual updates, and did not perform well in changing environments.

PhishGuard performs better in these aspects because it is lightweight and can learn automatically, allowing it to detect phishing attempts quickly. It can be used on different platforms, which makes it suitable for both individual users and organizations. It also provides clear and understandable feedback, which helps users trust the system more—something that was often missing in earlier research.[12]

3. Linking Accuracy with Practical Performance in Phishing Detection

PhishGuard shows a good balance between accuracy and overall system efficiency. Many existing approaches focus only on accuracy and ignore usability or system performance. However, PhishGuard shows that a good phishing detection system should be both accurate and practical to use. Because of this balance, it performs better than many existing solutions not only in testing environments but also in real-world use.[11]

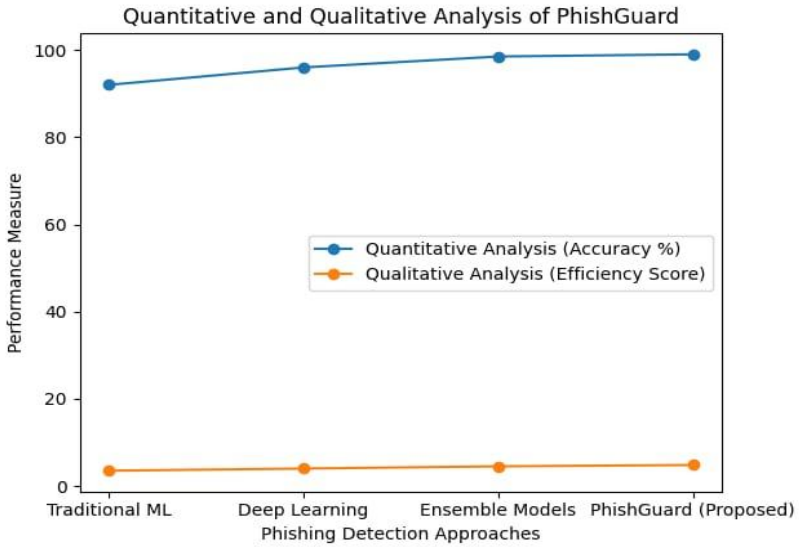


Figure 2. Performance Measures

3. System Architecture

3.1 Logical Flow

The PhishGuard system is designed to process data efficiently while providing quick and reliable results.

This system helps people stay safe from online scams. When a user checks an email or a website link, the system analyzes it step by step. It looks for warning signs such as unusual words, suspicious links, or abnormal website details. It then compares the data with previous examples of real and phishing messages to determine the risk level. Based on this analysis, it estimates how risky the email or website is. In the end, it clearly tells the user if it is safe, suspicious, or a phishing attempt, so they can avoid being tricked.

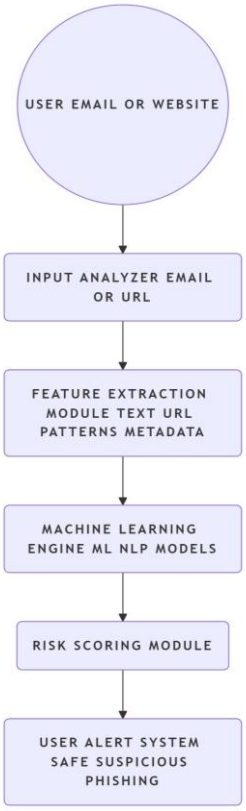


Figure 3. Logical Flow

3.2 Detection Model

This diagram shows the step-by-step process of phishing detection. It starts when the system receives an email or a website link. The system then divides the content into smaller parts for analysis. It identifies important features such as suspicious words or patterns and converts them into a format suitable for analysis. The processed data is then evaluated by a trained model to determine the level of risk. The result is compared with a predefined threshold to make a final decision. In the final step, the system informs the user whether the email or website is safe, suspicious, or a phishing attempt.

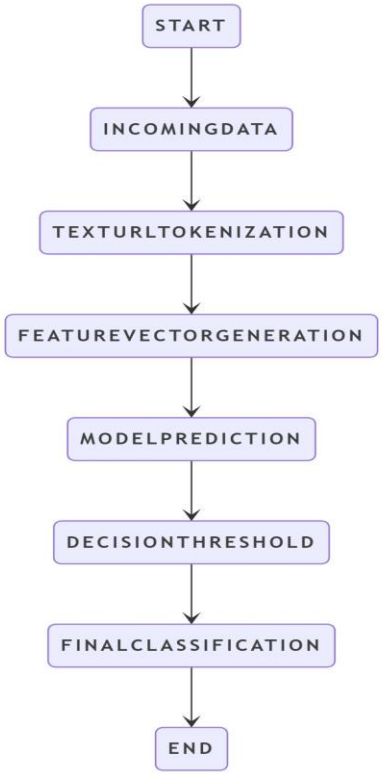


Figure 4. Modular Flow

3.3 Challenges in Designing the PhishGuard System

While developing PhishGuard, we faced several challenges:
• **Dataset Availability:** It was difficult to find reliable and recent phishing datasets because attack methods keep changing frequently.
• **False Positives:** It was challenging to correctly identify phishing emails without mistakenly warning users about safe emails.
• **Real-Time Processing:** Designing the system to be both fast and accurate was not easy and required careful planning.
• **Explainability:** It was also difficult to make the alerts simple enough for non-technical users to understand.
• **Generalization:** Another challenge was building a model that can handle different types of phishing attacks and work across multiple languages.

4. Advantages and Limitations

4.1 Advantages

- The system can detect phishing attempts instantly as emails or links are checked.
- It can identify newly created phishing attacks that are not yet listed in existing databases.
- The system provides simple and easy-to-understand alerts for users.

- It is designed to run efficiently without using too many system resources and can handle increasing data when needed
- The system can be easily connected with email applications and web browsers for practical use.

4.2 Limitations

- The accuracy of the system largely depends on the quality and diversity of the data used for training.
- Setting up the system and training the model can be difficult and may require technical knowledge.
- The system may not always detect advanced or well-crafted phishing attacks that closely resemble legitimate messages
- The system needs regular updates to stay effective against new and evolving phishing techniques.

5. Result

After going through different studies, it's clear that systems work best when they can keep watching things all the time and react quickly. For our topic, PhishGuard, this means continuously checking emails and websites for any suspicious activity. Instead of waiting for an attack to happen, it can stop it right at the beginning. This makes users feel safer while using online platforms. In simple words, a fast and alert system like PhishGuard can protect people better and build trust in the digital world.

6. Discussion

Phishing attacks are everywhere, trying to trick people into giving away personal information. Most traditional security systems can't catch these attacks quickly enough..PhishGuard helps by spotting phishing emails and fake websites in real time..It looks at things like links, who sent the message, and what the content says. As soon as it detects something suspicious, it warns the user immediately. It keeps learning new tricks that hackers use, so it stays up to date. Companies can use it to protect their employees and important data. It also teaches users to recognize phishing, making everyone more careful online..In the future, it could expand to mobile apps and social media monitoring. Overall, PhishGuard acts like a smart guard, keeping users safe from online scams.

7. Conclusions

- PhishGuard was selected as a research topic because phishing attacks have been increasing rapidly in recent years. As more services move online, many users with limited cybersecurity awareness become easy targets. This work aims to improve online safety by providing users with real-time protection and better awareness.[1]

- In the future, PhishGuard can be expanded to work on mobile devices, browser extensions, and larger organizational systems. Further improvements may include the use of advanced deep learning techniques and behavior-based analysis to handle new types of phishing attacks. Overall, PhishGuard is a step toward building more effective and practical cybersecurity solutions..[1].

8. Future Scope

In the future, PhishGuard can become even smarter and more helpful by using advanced AI to catch tricky phishing attacks that are hard to notice. It can slowly grow to protect not just emails, but also messages, social media, and even phone calls. The system may understand normal user behavior and quickly warn if something feels unusual. It could work smoothly with browsers and email apps so users stay protected without doing anything extra. It can also explain warnings in a simple way so users understand what went wrong. Overall, PhishGuard can become like a personal security assistant that keeps users safe in their daily digital life.

References

[1] M. Jakobsson and S. Myers, *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. Hoboken, NJ, USA: Wiley, 2006.

[2] R. A. Grimes, *Fighting Phishing: Everything You Can Do to Fight Social Engineering and Phishing*. Hoboken, NJ, USA: Wiley, 2023.

[3] P. Cassidy, S. W. Ellis, R. Woodford, and T. Hamilton, "APWG phishing activity trends report," Anti-Phishing Working Group (APWG), Mar. 2025. [Online]. Available: https://apwg.org. [Accessed: Jul. 28, 2026].
[4] E. Schechter and A. Wozniak, "Google Safe Browsing documentation," Google Developers, Sep. 2024. [Online]. Available: https://developers.google.com/safe-browsing. [Accessed: Jul. 28, 2026].
[5] F. Pedregosa *et al*., "Scikit-learn: Machine learning in Python," *J. Mach. Learn. Res.*, vol. 12, pp. 2825–2830, 2011. [Online]. Available: https://scikit-learn.org/stable/user_guide.html. [Accessed: Jul. 28, 2026].
[6] R. Mohammad, F. Thabtah, and L. McCluskey, "Phishing websites data set," UCI Machine Learning Repository, Univ. California, Irvine, CA, USA, Mar. 2015. [Online]. Available: https://archive.ics.uci.edu/ml. [Accessed: Jul. 28, 2026].
[7] OWASP Foundation, "Phishing," OWASP Web Community, Apr. 21, 2020. [Online]. Available: https://owasp.org/www-community/attacks/Phishing. [Accessed: Jul. 28, 2026].
[8] S. Bird, E. Loper, and E. Klein, *Natural Language Toolkit (NLTK)*, 2001. [Online]. Available: https://www.nltk.org/documentation.html. [Accessed: Jul. 28, 2026].
[9] P. Janani, K. Shri Varshini, and S. Vasundhara, "A phishing URL detection tool PhishGuard using Python," Apr.–Jun. 2025.
[10] "Phishing detection: A literature survey," [Online]. Available: https://www.researchgate.net/publication/256841808_Phishing_Detection_A_Literature_Survey.
[11] "Phishing detection using machine learning algorithm," [Online]. Available: [Publication details and URL to be added].
[12] K. K. Reddy, "Detection of phishing websites using a machine learning approach," *International Journal of Advanced Research, Ideas and Innovations in Technology*, [vol.], no. [no.], pp. [pages], [year].
[13] "Detection of phishing using machine learning algorithms," *International Journal of Computational Learning & Intelligence*, vol. [vol.], no. [no.], pp. [pages], [year].
[14] "A high-accuracy phishing website detection method based on machine learning," *ScienceDirect*, [journal title], vol. [vol.], no. [no.], pp. [pages], [year].
[15] "Phishing website detection based on effective machine learning approach," *Journal of Cyber Security Technology*, vol. 5, no. 1, pp. [pages], [year].
[16] "Machine learning-based phishing detection system," *International Journal of Intelligent Systems and Applications in Engineering*, vol. [vol.], no. [no.], pp. [pages], [year].
[17] "Phishing website detection and analysis using machine learning," *International Journal of Integrated Science and Technology*, vol. [vol.], no. [no.], pp. [pages], [year].
[18] "Malicious URL detection using machine learning: A survey," *arXiv preprint arXiv:1701.07179*, Jan. 2017.
[19] "Phishing attacks detection—A machine learning-based approach," *arXiv preprint arXiv:2201.10752*, Jan. 2022.
[20] "Machine learning approach for phishing website detection: A literature survey," [Publication details to be added].
[21] "High accuracy phishing detection based on convolutional neural networks," *arXiv preprint arXiv:2004.03960*, Apr. 2020.
[22] "Detecting phishing sites—An overview," *arXiv preprint arXiv:2103.12739*, Mar. 2021.
[23] "A case study on phishing detection with a machine learning net," *International Journal of Data Science and Analytics*, Springer, vol. [vol.], no. [no.], pp. [pages], [year].
[24] "A survey of phishing attacks: Their types, vectors and technical approaches," *ScienceDirect*, [journal title], vol. [vol.], no. [no.], pp. [pages], [year].
[25] "A survey of intelligent detection designs of HTML URL phishing attacks," [Publication details to be added].
[26] "Phishing detection techniques: A review," [Publication details to be added].
[27] R. Anderson, *Security Engineering*, 3rd ed. Hoboken, NJ, USA: Wiley, 2020.
[28] "Detection of phishing websites using machine learning," in *Proc. IEEE [Conference Name]*, [year], pp. [pages].
[29] "Phishing detection: A literature survey," *IEEE [Journal/Magazine Title]*, vol. [vol.], no. [no.], pp. [pages], [year].
[30] S. Khandelwal and R. Das, *Phishing Detection Using Content-Based Image Classification*. London, U.K.: Routledge, 2021.
[31] O. A. Akanbi, I. S. Amiri, and E. Fazeldehkordi, *A Machine-Learning Approach to Phishing Detection and Defense*. Amsterdam, Netherlands: Elsevier, 2020.
[32] A. Elhanashi, P. Dini, *et al*., *Machine Learning for Cybersecurity: Threat Detection and Mitigation*. Cham, Switzerland: Springer, 2022.