ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

REAL-TIME AIML BASED PHISHING DETECTION AND PREVENTION SYSTEM

[1]Mr. T. SeshaSai,[2]Manyam Kusumanjali,[3]Kathi Nissy Ronald,[4]Kolluri Jaya Krishna

[1]Assistant Professor, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

[2,3,4]U. G Student, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

ABSTRACT-*This project presents a Real-Time AI/ML-Based Phishing Detection and Prevention System that enhances cybersecurity by identifying and preventing phishing websites. The system uses Artificial Intelligence (AI) and Machine Learning (ML) techniques to analyze URLs and classify them as legitimate or phishing in real time. It provides users with instant security analysis, risk level, risk percentage, and recommendations before they access suspicious websites. Traditional phishing detection methods mainly rely on blacklists and manual verification, which are often unable to detect newly created phishing websites and zero-day attacks. These approaches may result in delayed detection and increased risk of credential theft, financial fraud, and data breaches. Therefore, there is a need for an intelligent, real-time, and cost-effective phishing detection system that can accurately identify malicious websites and help users browse the internet safely. The proposed system provides a secure, scalable, and user-friendly solution for improving online security and protecting users from phishing attacks.*

KEYWORDS: *Artificial Intelligence (AI), Machine Learning (ML), Phishing Detection, Cybersecurity, URL Analysis, Real-Time Detection, Feature Extraction, Website Security.*

INTRODUCTION

The internet has become an essential part of everyday life, allowing people to access online banking, shopping, education, and communication services. However, the increasing use of the internet has also led to a

rise in phishing attacks, where fake websites are created to steal sensitive information such as usernames, passwords, banking details, and personal data. With advancements in Artificial Intelligence and Machine Learning, phishing detection has become faster and more accurate. This project combines AI-based phishing detection with a web application to improve online security and protect users from malicious websites. The proposed system not only detects phishing websites in real time but also provides risk analysis and security recommendations, helping users browse the internet safely and confidently.

LITERATURE SURVEY

Phishing attacks have become one of the most common cybersecurity threats due to the rapid growth of internet services and online transactions. Phishing websites are designed to imitate legitimate websites and deceive users into revealing sensitive information such as usernames, passwords, banking credentials, and personal data. Traditional detection methods, such as blacklists and manual verification, are often unable to detect newly created phishing websites in real time.

To overcome these limitations, researchers have explored the use of Artificial Intelligence and Machine Learning techniques for phishing detection. These intelligent approaches analyze URL patterns, website features, and user behavior to accurately identify phishing websites, improving online security and helping users browse the internet safely.

RELATED WORK

Several researchers have contributed to the development of AI and Machine Learning-based phishing detection systems to improve online security and protect users from cyber threats. Early phishing detection methods mainly relied on blacklist databases, rule-based techniques, and manual verification. Although these approaches were effective against known phishing websites, they were unable to detect newly created.

EXISTING SYSTEM

The existing phishing detection systems mainly rely on blacklists, rule-based methods, and manual verification to identify malicious websites. These methods are effective only for detecting previously known phishing websites and often fail to identify newly created or zero-day phishing attacks. Many traditional systems require frequent database updates and cannot provide real-time protection against evolving cyber

threats. They also offer limits accuracy when attackers use advanced techniques to create phishing websites that closely resemble legitimate ones. Overall, the existing systems lack intelligent analysis, real-time detection, and the ability to effectively detect new and sophisticated phishing attacks.

PROPOSED SYSTEM

The proposed system implements an AIML-based phishing detection to identify malicious websites in real time. It analyzes website URLs by extracting important features and classifies them as Safe or Phishing using a trained Machine Learning model. The system provides users with instant results, including the website status, risk level, risk percentage, and security recommendations. This approach helps users avoid phishing websites before sharing sensitive information, thereby reducing the risk of cyberattacks and online fraud. The application provides a secure login system, stores URL scan history in a database for future references, and offers a simple, user-friendly web interface. Its scalable architecture also supports future enhancements such as browser extensions, email phishing detection, QR code scanning, and real-time threat intelligence integration.

SYSTEM ARCHITECTURE

The architecture of the Real-Time AI/ML-Based Phishing Detection and Prevention System consists of a user interface, Machine Learning model, Flask backend, feature extraction module, database, and result display module, The user first login and then enters a website URL through the web interface, which is then sent to the Flask backend for processing.

The feature extraction module extracts important URL characteristics and passes them to the training Machine Learning model The model analyzes these features and classifies the website as Safe or Phishing. Based on the prediction, the system displays the website status, risk level, risk percentage, and security recommendations to the user. The scanned URL and prediction results are securely stored in the database, allowing users to view their scan history and analytics. This architecture provides fast accurate, and real-time phishing detection, helping users browse the internet safely and securely.

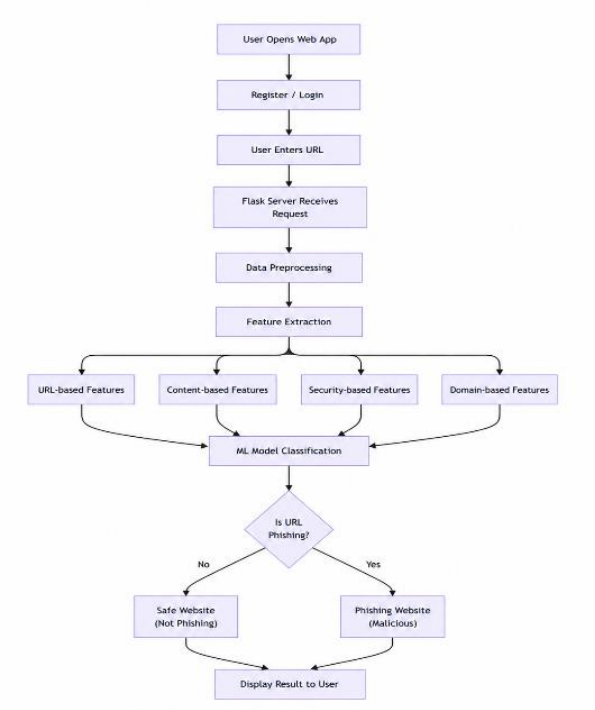


Fig 1: System Architecture

METHODOLOGY DESCRIPTION

The methodology of the Real-Time AIML-Based Phishing Detection and Prevention System is designed to identify phishing websites quickly and accurately using Artificial Intelligence and Machine Learning techniques. The system follows a structured approach that includes URL input, feature extraction, Machine Learning-based classification, result generation, and secure data storage. This process enables real-time phishing detection while providing users with websites status, risk level, risk percentage, and security recommendations, ensuring safe and secure internet browsing.

RESULTS AND DISCUSSION

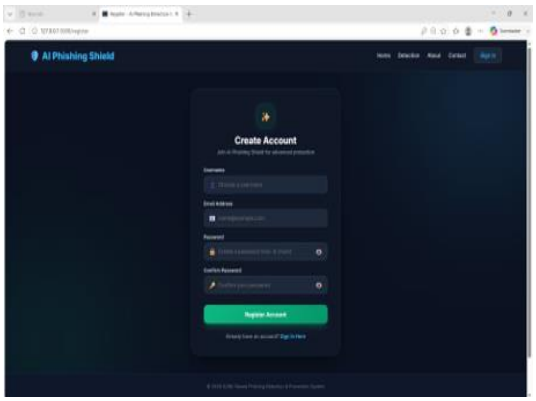


Fig 1: Register Page

Allows new users to create an account by entering their username, email, and password to access the phishing detection system.

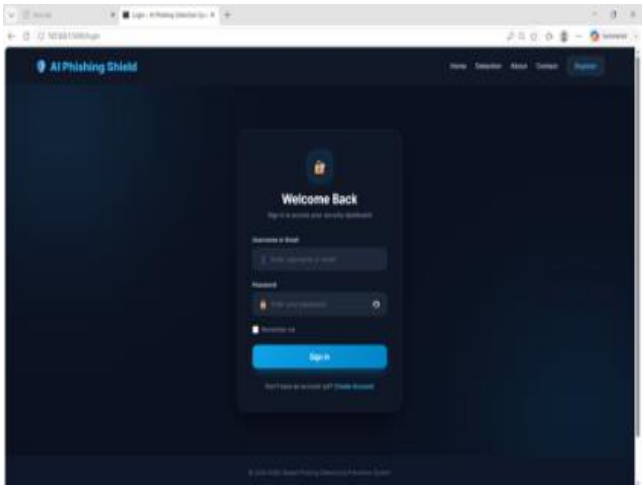


Fig 2: Login Page

Authenticates registered users using their credentials and provides secure access to the application dashboard.

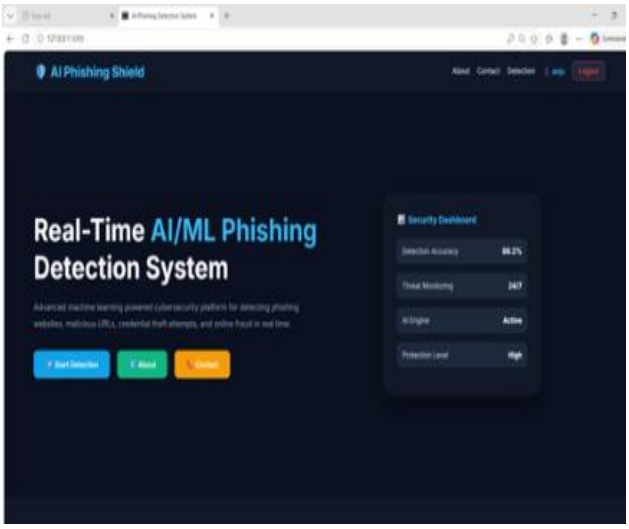


Fig 3: Home Page

Displays the project overview and provides navigation to phishing detection, analytics, and other system features

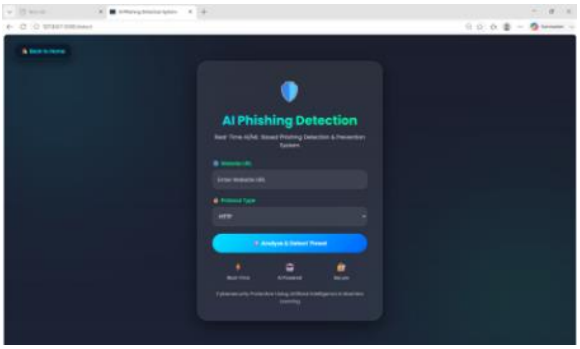


Fig 4: URL Detection Page

Accepts a website URL and protocol from the user to analyze the link using the AI/ML phishing detection model.

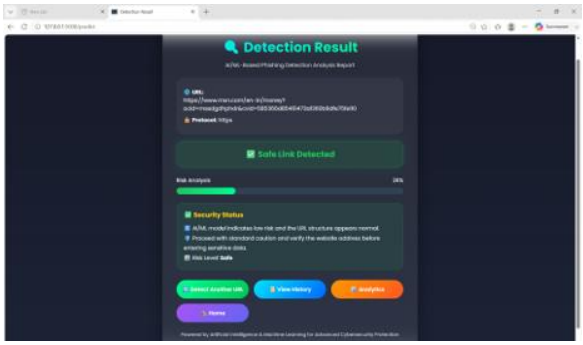


Fig 5: Safe Link Result Page

Shows that the submitted URL is legitimate with a low-risk score and recommends safe browsing practices.

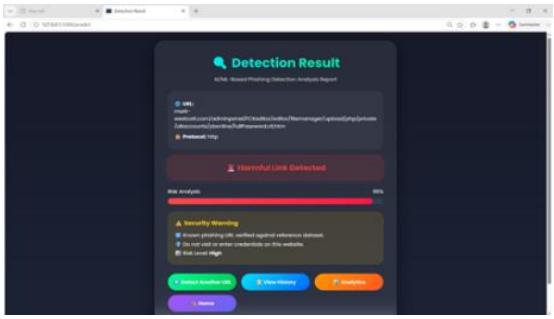


Fig 6: Phishing Link Result Page

Identifies the submitted URL as a phishing website with a high-risk score and warns users to avoid accessing it.

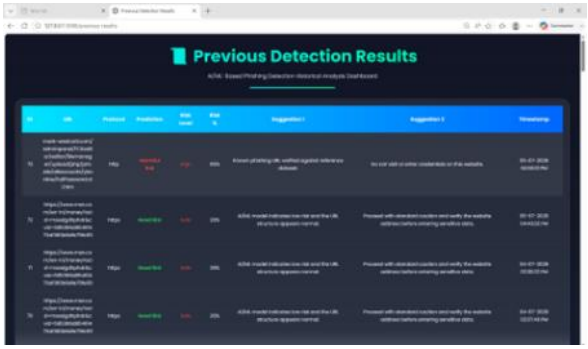


Fig 7: History Page

Displays the history of previously analyzed URLs along with prediction results, risk levels, and timestamps.



Fig 8: Analytics Dashboard

Visualizes phishing detection statistics, risk distribution, and trend analysis using interactive charts and performance metrics.

CONCLUSION

The Real-Time AIML-Based Phishing Detection and Prevention System enhances online security by accurately detecting phishing websites using Artificial Intelligence and Machine Learning. By identifying malicious URLs in real time and providing risk analysis and security recommendations, the system helps usres avoid cyber threats and protect sensitive information. It offers a secure, reliable, and user-friendly solution for safe internet browsing while improving cybersecurity awareness and reducing the risk of phishing attacks.

FUTURE SCOPE

The proposed Real-Time AI/ML-Based Phishing Detection and Prevention System can be furthur enhanced by intigrating advanced Deep Learning models to improve phishing detection and reduce false predictions. The system can be extended to detect email phishing, QR code phishing, and malicious attachments for broader cybersecurity protection.

It can also support cloud deployment, browser extensions, and mobile applications for real-time phishing detection across multiple platforms. Additionally, integration with real-time threat intelligence services and automated security alerts can further strengthen online security and help users respond quickly to emerging cyber threat.

REFERENCES

[1] P. Harini, “Sms based wireless e-notice board,” *International Journal of Emerging Technology and Advanced Engineering,* vol. 3, no. 3, pp. 181-185, 2013.

[2] P. Harini, “Enhanced packet delivery techniques using crypto-logic riddle on jamming attacks for wireless communication medium,” *Int. J. Latest Trends Eng. Technol,* vol. 2, no. 4, pp. 469-478, 2013.

[3] P. Harini, "[Retracted] Machine Learning Algorithms Are Applied in Nanomaterial Properties for Nanosecurity," *Journal of Nanomaterials,* vol. 2022, no. 1, p. 5450826, 2022.

[4] Abdillah, R., & Syafitri, W. (2024). Phishing Detection in Deep Learning: Systematic Literature Review. Jurnal CoreIT.

Link:https://ejournal.uinsuska.ac.id/index.php/coreit/article/view/31009

5] Patil, K., & Bhatt, V. (2025). Anti-Phishing Frameworks for Safer Digital Ecosystems: A Systematic Review. Journal of Cyber Security, Privacy Issues and Challenges.

Link: https://matjournals.net/engineering/index.php/JCSPIC/article/view/3146

[6] Catal, C., Giray, G., Tekinerdogan, B., Kumar, S., & Shukla, S. (2022). Applications of Deep Learning for Phishing Detection: A Systematic Literature Review. Knowledge and Information Systems.

Link:https://pubmed.ncbi.nlm.nih.gov/35645443/

[7] Ige, T., Kiekintveld, C., Piplai, A., Waggler, A., Kolade, O., & Matti, B. H. (2024). An Investigation into the Performances of State-of-the-Art Machine Learning and Deep Learning Classifiers for Phishing Detection: A Survey. arXiv.

Link: https://arxiv.org/abs/2411.16751

[8] Newaz, A., Haq, F. S., & Ahmed, N. (2024). A Sophisticated Framework for the Accurate Detection of Phishing Websites. arXiv.

Link: https://arxiv.org/abs/2403.09735

[9] Kulkarni, A., Balachandran, V., Divakaran, D. M., & Das, T. (2024). From ML to LLM: Evaluating the Robustness of Phishing Webpage Detection Models Against Adversarial Attacks. arXiv.

Link: https://arxiv.org/abs/2407.20361

[10] Jackson, K. A. (2023). A Systematic Review of Machine Learning Enabled Phishing. arXiv.

Link: https://arxiv.org/abs/2310.06998

[11] El-Maghraby, A., et al. (2024). Deep

Learning-Based Phishing Detection Techniques: Recent Advances and Challenges. Electronics (MDPI).

Link:https://www.mdpi.com/2079-9292/13/19/3823

[12] Wilk-Jakubowski, J. Ł., et al. (2025). Recent Trends in Machine Learning-Based Phishing Detection. Electronics (MDPI).

Link:https://www.mdpi.com/2079-9292/14/18/3744

[13] Abdillah, R., & Syafitri, W. (2024). Deep Learning Techniques for Phishing Detection: Current Research and Future Directions. Jurnal CoreIT.

Link:https://ejournal.uin-suska.ac.id/index.php/coreit/article/view/31009

[14] Patil, K., & Bhatt, V. (2025). Machine Learning and Ensemble Models for Phishing Website Detection: A Systematic Review. Journal of Cyber Security, Privacy Issues and Challenges.
Link:
https://matjournals.net/engineering/index.php/JCSPIC/article/view/3146

[15] Daoud, E., Garcia-Blas, J., & Carretero, J. (2025). Machine Learning Techniques for Phishing Website Detection: A Comprehensive Survey. IEEE Access.

Link: https://ieeexplore.ieee.org/