JVM's Mehta Degree College, Sector 19, Airoli
NAAC Re-accredited "A+" Grade
IQAC in association with Western Regional Centre, ICSSR Organized one day National Conference on "Integrating Multidisciplinary Approaches to Build a Resilient and Sustainable Future", held on 10th January 2026

MACHINE LEARNING APPROACHES FOR DETECTING PHISHING ATTACKS IN REAL-TIME

[1]Laxmi Dinanath Yadav and [2]Sharayu Kadam
[1]M.Sc. IT Student, Jnan Vikas Mandal's College, Airoli, Thane, Maharashtra
[2]Assistant Professor, Department of Information Technology Jnan Vikas Mandal's College, Airoli.

ABSTRACT

Phishing attacks have become one of the most prevalent cybersecurity threats, causing significant financial and reputational losses. These attacks often use deceptive emails, websites, or messages to trick users into revealing sensitive information. Traditional detection methods rely on static blacklists and rule-based systems, which are insufficient for real-time threats. This research explores the application of machine learning techniques for detecting phishing attacks in real-time. Various algorithms, including Decision Trees, Random Forest, Support Vector Machines, and Neural Networks, are evaluated for their effectiveness in identifying phishing URLs and emails. The methodology involves data collection from publicly available datasets, preprocessing, feature extraction, and model training.

Performance is measured using evaluation metrics including accuracy, precision, recall, and the F1-score. Results indicate that machine learning models, particularly ensemble approaches like Random Forest, can significantly improve detection rates while minimizing false positives. The study demonstrates that integrating these models into real-time monitoring systems can enhance cybersecurity defences and reduce user vulnerability. This paper also highlights limitations, including data imbalance and evolving attack strategies, and suggests future work for adaptive and automated systems capable of continuous learning.

Keywords: *Machine Learning, Phishing Detection, Real-Time, Cybersecurity, Decision Trees, Random Forest, SVM*

INTRODUCTION

Phishing attacks are cyber threats designed to deceive users into disclosing confidential information, such as login credentials, banking details, or personal data. These attacks are often carried out via emails, social media messages, or fraudulent websites. The rapid increase in internet users and online services has made phishing attacks more sophisticated and difficult to detect. Traditional security solutions, such as blacklists, heuristic rules, and signature-based detection, are often reactive and fail to respond to newly emerging threats. Consequently, there is a growing need for proactive, intelligent systems capable of identifying phishing attempts in real-time. Machine learning (ML) has proven to be an effective solution for tackling this problem. By learning patterns from historical phishing data, ML models can automatically classify URLs, emails, and messages as legitimate or malicious. This research focuses on exploring various ML algorithms for real-time phishing detection, comparing their effectiveness, and demonstrating their potential in strengthening cybersecurity frameworks. The study also emphasizes practical implementation considerations for deploying ML models in real-time environments.

LITERATURE REVIEW

Previous research in phishing detection has focused on several approaches, including heuristic-based, blacklist-based, and machine learning-based methods. Heuristic approaches rely on predefined rules to identify suspicious patterns in emails and URLs. While effective against known attacks, they fail against evolving phishing techniques. Blacklist-based systems maintain databases of malicious URLs but cannot detect newly created phishing sites. Machine learning approaches have demonstrated significant improvements in detection accuracy and adaptability. Researchers have applied supervised learning algorithms, such as Decision Trees, Random Forests, Support Vector Machines (SVM), and Naïve Bayes, to classify phishing content. Deep learning techniques, including neural networks, have also shown promise in identifying complex patterns in textual and URL features. Studies indicate that ensemble methods, such as Random Forest and Gradient Boosting, outperform individual models in terms of accuracy and robustness. Additionally, real-time detection systems leverage streaming data to continuously monitor network traffic, emails, and websites, enabling rapid response to phishing attempts. Despite advancements, challenges remain, including feature selection, data imbalance, and maintaining low false-positive rates in dynamic online environments.

RESEARCH OBJECTIVES

The primary objective of this research is to develop and evaluate machine learning models capable of detecting phishing attacks in real-time. The specific aims include:

- To collect and preprocess phishing datasets from publicly available sources.
- To evaluate and compare the performance of these models using metrics such as accuracy, precision, recall, and F1-score.
- To design a framework for real-time phishing detection suitable for integration into IT security systems.
- To identify limitations and propose improvements for adaptive and automated phishing detection systems.

METHODOLOGY

The research methodology involves several key steps:

- **Data Collection:** Public datasets, including Phish Tank, Open Phish, and custom-collected phishing emails and URLs, are used. Legitimate URLs and emails are collected from trusted sources to create a balanced dataset.
- **Data Preprocessing:** The datasets undergo cleaning to remove duplicates, handle missing values, and encode categorical features. Feature extraction focuses on URL characteristics (length, presence of special characters, domain age), email metadata, and textual patterns.

Machine Learning Models:

- **Decision Tree:** A tree-based model that splits data based on feature thresholds to classify phishing and legitimate instances.
- **Random Forest:** A combination of several decision trees designed to enhance accuracy and minimize overfitting.
- **Support Vector Machine (SVM):** A model that identifies an optimal hyperplane to separate phishing and legitimate instances.
- **Neural Networks:** Deep learning model capable of capturing complex patterns in data.

Model Training and Evaluation: The dataset is split into training and testing sets. Cross- validation ensures robust performance assessment. Evaluation metrics include accuracy, precision, recall, and F1-score.

Real-Time Detection Framework: The selected model can be deployed in a streaming environment, monitoring URLs or emails as they arrive, classifying them, and triggering alerts in case of phishing detection.

CONCLUSION

This research demonstrates that machine learning models are effective in detecting phishing attacks in real-time. Among the algorithms tested, ensemble methods like Random Forest achieved the highest accuracy and low false-positive rates. The study highlights that integrating ML models into real-time monitoring systems enhances cybersecurity by providing proactive detection of malicious content. Challenges such as data imbalance, feature selection, and evolving phishing tactics require ongoing research and adaptation.

Future work can focus on developing adaptive learning systems that continuously update models with new phishing patterns and integrate natural language processing for email content analysis. Implementing these solutions can significantly reduce the risk posed by phishing attacks, protecting both individuals and organizations.

REFERENCES

[1] S. Abu-Nimeh, D. Nappa, X. Wang, and S. Nair, “Comparison of Various Machine Learning Techniques for Detecting Phishing Attacks,” eCrime Researchers Summit, 2007.

[2] A. Bergholz, J. De Beer, S. Glahn, M. Moens, G. Paaß, and S. Strobel, “Innovative Filtering Methods for Phishing Emails,” Journal of Computer Security, vol. 18, no. 1, pp. 7– 35, 2010.

[3] M. Khonji, Y. Iraqi, and A. Jones, “A Survey on Phishing Detection Techniques,” IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2091–2121, 2013.

[4] A. Jain and B. B. Gupta, “Analysis of Features and Methods for Phishing Detection,” Procedia Computer Science, vol. 132, pp. 1045–1053, 2018.

[5] Y. Zhang, J. Hong, and L. F. Cranor, “Cantina: Detecting Phishing Websites Using Content-Based Approaches,” WWW Conference, 2007.