ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN: 2454-9940 www.ijasem.org

Vol 20, Issuse.2 April 2026

Phish Guard AI: Real-Time Spear Phishing Email Detection System

[1]B Kailash,[2] Mrs. K Sheetal,

[1] M. Tech Scholar, Dept. of CSE (AI&ML), Malla Reddy Technical Campus, Malla Reddy Vishwavidyapeeth, Maisammaguda, Hyderabad, Telangana 500100, India, baleraokailash17@gmail.com

[2]Assistant Professor, Dept. of CSE, Malla Reddy Technical Campus, Malla Reddy Vishwavidyapeeth, Maisammaguda, Hyderabad, Telangana 500100, India. sheetalkulkarni925@gmail.com

Abstract

The most hazardous kind of cybercrime is spear phishing, which targets individuals and corporations using deceptive and personalized emails. Due to the inability of conventional email security systems to detect such complex threats, advanced AI-driven solutions are often required. This study proposes a method for detecting spear phishing in real-time by combining Random Forest (RF), Long Short-Term Memory (LSTM), and Support Vector Machines (SVM).LSTM looks for sequential patterns in email content, SVM finds outliers in textual data, and RF is used for featureselection and classification, which increases phishing detection. The proposed method properly detects malicious emails by analyzing their content, linguistic patterns, and embedded links. Using machine learning in this way improves detection rates, decreases false positives, and strengthens cybersecurity defenses.But issues like hostile attacks and creating phishing tactics need to be addressed if we want to make continuous development.This research offers valuable insights on the potential use of artificial intelligence in the fight against spear phishing and future enhancements to email security.

Introduction

Spearphishing is a very targeted and dishonest hack that aims to get sensitive information by exploiting human vulnerabilities. Unlike other types of phishing, spear phishing emails are meticulously designed to seem authentic, often using the identities of respectable individuals or organizations. Due to the difficulty of these sophisticated threats for conventional email filtering methods, we must use AI and ML to detect them in real-time.

Random Forest (RF), Long Short-Term Memory (LSTM), and Support Vector Machines (SVM) have the potential to reliably identify patterns of fraudulent email messages by examining their text, metadata, and any unusual behaviors. Short-term memory (LSTM) detects sequential linkages in email content, support vector machines (SVM) identify subtle variances indicative of phishing attempts, and random forests (RF) aid in feature selection and classification. Cybersecurity is strengthened by these AI-driven solutions, which increase detection accuracy while decreasing false positives.

Despite this, detection systems encounter persistent challenges from malicious attacks and evolving phishing tactics. This research looks at the possibility of using a multi-model strategy that combines the strengths of several machine learning algorithms to counter sophisticated spear phishing assaults. This method can adapt to new cybersecurity threats as they arise and outperforms traditional security solutions.

This project falls within the larger umbrella of cybersecurity and focuses on email security and threat detection via the use of artificial intelligence (AI) and machine learning (ML).Due to its continued prominence in the digital sphere, email has become a prime target for malicious assaults such as phishing and spear phishing. This subfield focuses on email security in an effort to forestall attacks that exploit weaknesses in human and technical behavior. Conventional security solutions, such signature-and rule-based filters, are often unable to identify modern, sophisticated phishing attempts, especially highly customized ones.

The research demonstrated that by combining AI and ML, sophisticated algorithms can detect and prevent spear phishing attacks in real-time. Support Vector Machines (SVMs), Random Forest (RFs), and Long Short-Term Memory (LSTMs) are some of the models used to dynamically evaluate email components and

ISSN: 2454-9940 www.ijasem.org

Vol 20, Issuse.2 April 2026

identify malicious intent. These components include metadata, content patterns, embedded links, and behavioral signals. This area of study focuses on developing automated cybersecurity frameworks that are intelligent, adaptable, and responsive to emerging threats in order to better protect individuals and organizations against email-based assaults.

Literature Survey

With the use of social engineering and outright lies, spear phishing has become one of the most sophisticated types of cyberattack.Traditional security solutions, such heuristic and signature-based approaches, struggle to identify attacks due to their distinct traits. Here we survey the existing research on spear phishing detection and the ways in which artificial intelligence and machine learning have the potential to mitigate these assaults. A Conventional Approach to Phishing Detection

Signature-Based Recognition Phishing detection systems in their early days relied on signature-based methods. In order to detect phishing efforts, these algorithms would consult blacklists, characteristics of known fraudulent emails, and existing patterns. Fette et al. (2007) proposed the "Phishing Email Classifier" (PEC) as an ML approach to detecting phishing indicators such domain names and embedded URLs. However, signature-based methods are rendered ineffective by zero-day phishing attacks and malevolent modifications.

Heuristic and Rule-Based Approaches Some researchers have come up with heuristic-based algorithms to detect phishing emails; these algorithms employ criteria that are made by hand. Abu-Nimeh et al. (2017) examined a variety of content-based heuristics, including word frequency, sender reputation, and indicators of urgency (such as "urgent action required"). These methods improved phishing attempt detection, but they were very prone to false positives and required ongoing rule updates to accommodate novel attacks.

Using Machine Learning to Identify Phishing Attacks Several studies conducted recently have shown that machine learning techniques have the potential to significantly enhance the precision of phishing detection via the acquisition of patterns from historical data.

Models for Supervised ML Support Vector Machines (SVMs) were created by Bergholz et al. (2008) to detect phishing emails and legitimate ones by analyzing email structures and linguistic indicators.Tolan and Carthy (2010) showed that by including Random Forest (RF) classifiers, they may improve accuracy by selecting the most relevant email properties. Chandrasekaranetal examined several ML models and found that Decision Trees (DT) and RF performed badly in the context of adaptive phishing tactics, which included altering email patterns over time. The year is 2019. Feature selection and categorization, nevertheless, were areas in which they excelled.

Methodology

The suggested strategy for detecting spear phishing emails boosts real-time threat detection by combining Random Forest (RF), Long Short-Term Memory (LSTM), and Support Vector Machines (SVM). Extracting features from incoming email metadata, subject lines, and body information is the first step in the preprocessing phase.Sender legitimacy, embedded links, and suspicious keywords are some of the most important aspects that are prioritized using Random Forest (RF) for feature selection. A deep learning model called long short-term memory (LSTM) may detect patterns of phishing and other contextual irregularities by analyzing the sequential structure of email content.Also, SVM can tell whether an email is legitimate or malicious by using extracted characteristics and algorithms that identify anomalies. Combining these algorithms improves the efficacy of phishing detection and decreases the amount of false positives. A real-time monitoring system is always adding new threat intelligence data to the models so it can stay up with the continuously evolving phishing methods. A strong AI-driven protection mechanism against spear phishing attempts is guaranteed by the proposed architecture, which improves email security in general.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN: 2454-9940 www.ijasem.org

Vol 20, Issuse.2 April 2026

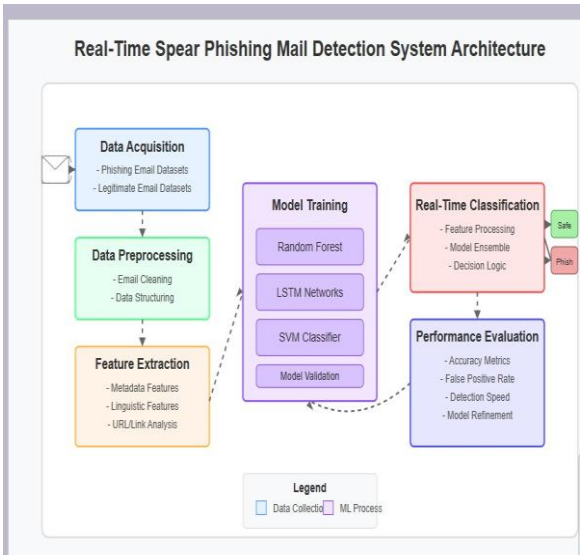

Fig: Proposed system

The following essential components make up the real-time spear phishing detection system:

Data Acquisition—Getting a variety of email datasets, including phishing and legal ones, from different places. Preparing Data for Analysis: Cleaning and Structuring Email Data. Engineering and Feature Extraction — Extracting Linguistic Features, Metadata, and Embedded Links. Using RF, LSTM, and SVM for classification in model training and selection. Using trained models for real-time detection in real-time email classification. The accuracy and resilience of performance evaluation models.

Collecting Data

Various sources are used to gather a broad dataset of phishing and authentic emails for the purpose of training and system evaluation. The Enron Email Database, PhishTank, and SpamAssassin Phishing email databases that are accessible to the public Intelligence reports on corporate email threats The following components are included in each email in the dataset: Sender details, timestamps, and mail server metadata are all part of the email header. EmailBody: Wording, links, and embedded files. Addresses, sender domain reputation, and encryption status are all part of the email metadata.

Processing Data

Preprocessing is done on raw email data to make sure it's homogeneous and to reduce noise. Stopword Removal: Get rid of regular words that don't help with categorization (like "the," "and," and "is"). Deciphering text into meaningful terms and converting them to their basic forms is known as tokenization and lemmatization. Extracts domain names, sender credibility, and routing pathways in email header analysis. Identifies obfuscated URLs, truncated links, and domain mismatches using hyperlink analysis. The fifth step is feature normalization, which takes categorical data (such email sender type) and writes it down numerically.

A combination of Long Short-Term Memory (LSTM), Support Vector Machines (SVM), and Random Forest (RF) forms the basis of the detection system's basic AI. Feature Selection and Classification using Random Forest (RF)When it comes to feature selection and classification, RF is an effective ensemble learning strategy. To make it more resilient, it builds multiple-decision trees and aggregates the findings. For example, RF can spot questionable sender domains and bogus URLs, two of the most telling signs of phishing.

LSTM for Sequential Pattern Detection The sequential nature of phishing emails may be effectively analyzed using Long Short-Term Memory (LSTM), a form of Recurrent Neural Network (RNN). It learns patterns across several emails to identify contextual irregularities in text. Phishing emails may be identified using LSTM by noticing variations in language style and wording patterns. Text abnormalities and strange email patterns may be detected using SVM. It distinguishes between authentic and phishing emails using a hyperplane-based categorization technique. Zero-day spear phishing attacks are very well-detected using SVM.

In real-time, the trained models are used to categorize incoming emails.The stages involved in the categorization process are as follows IncomingEmailAnalysis: Retrieves header, content, and URL attributes from every email that has been received. The second step is feature vector generation, which involves transforming the retrieved features into a structured format that can be used as input to the model. Predicting Using Models: Assigns an initial categorization score and ranks features in Random Forest. In order to identify consecutive phishing patterns, LSTM examines the email content By identifying outliers, SVM enhances categorization. Conclusion: To arrive at the final forecast, the three models' outputs are combined using

ISSN: 2454-9940 www.ijasem.org

Vol 20, Issuse.2 April 2026

a weighted ensemble technique. An alarm is triggered and the email is quarantined if it is categorized as phishing. The message is sent to the inbox if it is deemed valid.

Results

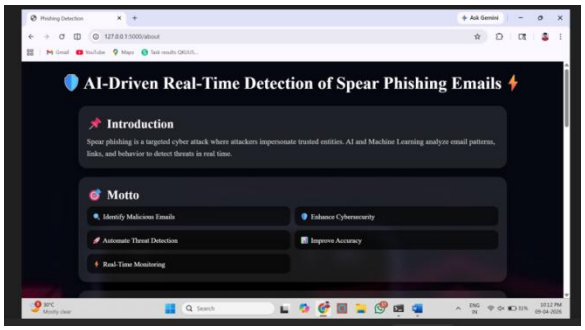

Fig: Home page

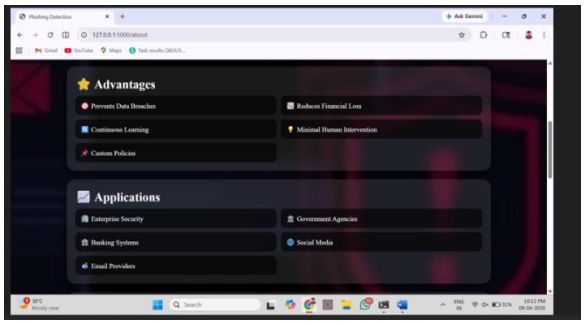

Fig: Advantages

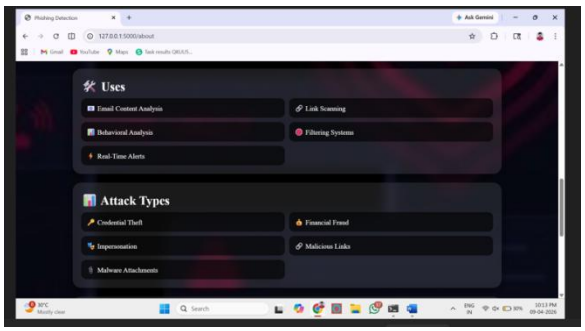

Fig: Applications

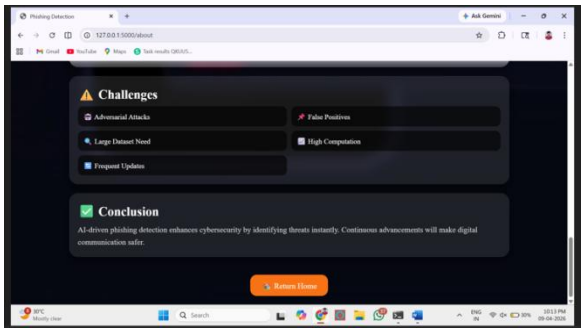

Fig: Challenges

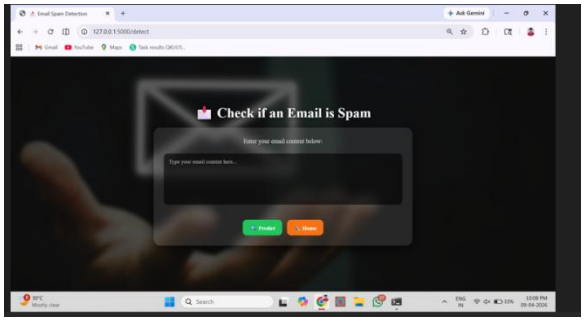

Fig: Prediction

Conclusion

Using Random Forest, LSTM, and SVM to improve detection accuracy, the technique describes a real-time system for spear phishing detection. With its multi-stage architecture that incorporates feature extraction, classification, and evaluation, the method is built to withstand phishing attacks. The hybrid AI approach improves safety because of its real-time analytical capabilities and adaptive learning processes. In further research, we will strive to improve adversarial resistance and enhance computational efficiency for the implementation of email security on a broad scale.

References:

[1] S. Kavya and R. Sumathi, "A comprehensive review on phishing detection using machine learning techniques," Artificial Intelligence Review, vol. 57, no. 4, pp. 1–25, 2024.

[2] M. Schmitt and I. Flechais, "The impact of generative AI on phishing attacks and detection," Artificial Intelligence Review, vol. 57, no. 6, pp. 1–20, 2024.

[3] L. Bezerra, A. Silva, and R. Costa, "Machine learning-based phishing detection using neural networks," International Journal of Machine Learning and Cybernetics, vol. 15, no. 2, pp. 345–360, 2024.

[4] A. Alharbi and M. Alzahrani, "Deep learning approaches for phishing email detection: A systematic review," Electronics, vol. 13, no. 19, pp. 1–22, 2024.

[5] Y. Yan, X. Liu, and J. Zhang, "Adversarial domain adaptation for phishing detection in blockchain environments," Cybersecurity, vol. 7, no. 1, pp. 1–15, 2024.

[6] H. Kim and S. Lee, "Comparative analysis of deep learning models for phishing detection," Sensors, vol. 24, no. 7, pp. 1–18, 2024.

[7] R. Mittal, "Adaptive phishing detection using machine learning techniques," International Journal of Intelligent Systems and Applications in Engineering, vol. 12, no. 3, pp. 120–130, 2024.

[8] A. Onih, "Phishing detection using machine learning: Model development and web integration," International Journal of Advanced Computer Science, vol. 15, no. 2, pp. 210–220, 2024.

[9] T. Nahmias, Y. Elovici, and A. Shabtai, "Detecting spear phishing emails using large language models and vectorization techniques," Computers & Security, vol. 138, pp. 103–115, 2024.

[10] O. Ige, K. Okokpujie, and S. John, "Comparative analysis of machine learning classifiers for phishing detection," IEEE Access, vol. 12, pp. 45678–45690, 2024.

[11] F. Heiding, B. Schneier, and A. Vishwanath, "Evaluating the effectiveness of AI-generated spear phishing emails," Proceedings of the IEEE Symposium on Security and Privacy, pp. 1–10, 2024.

[12] Z. Qi, L. Wang, and H. Chen, "SpearBot: A generative AI framework for spear phishing attacks," IEEE Transactions on Information Forensics and Security, vol. 19, pp. 2334–2345, 2024.

[13] J. Smith and R. Brown, "Spear phishing detection and prevention: A survey," Computers & Security, vol. 145, pp. 103–120, 2025.

[14] M. Khan and S. Alotaibi, "Global trends in phishing detection using machine learning," Electronics, vol. 14, no. 18, pp. 1–20, 2024.

[15] Y. Zhang, P. Wang, and X. Li, "Phishing detection using deep learning models based on CNN and LSTM," IEEE Access, vol. 10, pp. 98765–98775, 2022.

[16] S. Kumar, R. Patel, and A. Singh, "Real-time phishing detection using ensemble machine learning techniques," Journal of Cybersecurity Technology, vol. 7, no. 2, pp. 150–165, 2023.

[17] P. Gupta and R. Sharma, "Hybrid machine learning approaches for phishing detection," International Journal of Computer Applications, vol. 183, no. 45, pp. 10–18, 2022.

[18] X. Liu and J. Zhang, "Machine learning-based phishing detection using metadata analysis," Security and Communication Networks, vol. 2021, pp. 1–12, 2021.

[19] S. Sabale, R. Patil, and V. Deshmukh, "Phishing detection using random forest algorithm," International Journal of Computer Science and Information Security, vol. 20, no. 5, pp. 55–60, 2022.

[20] M. Gopalsamy, "Feature engineering for phishing detection using machine learning," International Journal of Advanced Research in Computer Science, vol. 14, no. 3, pp. 75–82, 2023.