International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

Reducing Phishing Attacks in Online Banking Using a Multi-Layered Machine Learning Framework

Nikhil Kumar, Shekhar Kumar Purbe, Dr. Jyoti Gautam
Sharda University Greater Noida

ABSTRACT—Phishing attacks are now considered to be the greatest cyber security threats in online banking, mobile wallet, and other online financial systems. Attackers launch such attacks not only exploit the vulnerabilities in systems but also exploit human factors to steal sensitive financial information and cause huge monetary losses and destroy users' credibility. Current defense strategies are blacklist based URL filtering and static rules based detection, which are unable to cope with modern phishing attacks. Modern phishing attacks are carried out by employing advanced techniques such as domain spoofing, adversary-in-the-middle (AiTM) attacks, and dynamic web contents . This paper proposes a multi-layered intelligent phishing detection architecture to defend online banking platforms. The proposed system uses URL analysis, content inspection, and transaction behavior analysis to protect online banking systems from different angles. The system uses machine learning algorithms such as Random Forest, Support Vector Machine, and Logistic Regression to classify phishing attacks based on the features extracted from URL, web pages, and user transactions. Unlike previous approaches which only use single layer detection, this paper proposes a hybrid system architecture with real-time detection and behavioral analysis to detect phishing attacks. The system is trained with datasets collected from multiple repositories which are publicly available phishing repositories. The experimental results show that the model trained by the proposed method achieves an accuracy of 96.5% with high precision and recall and low latency to be applied in real-time systems. The system also provides an alert and response mechanism to notify users and stop fraudulent transactions as soon as possible.

Keywords— Phishing Detection, Cybersecurity, Online Banking Security, Machine Learning, Multi-Layered Security Framework, URL Analysis, Content-Based Detection, Behavioral Analysis, Fraud Detection, Random Forest, Real- Time Detection, Financial Security.

I. INTRODUCTION

Blazing speed of digital technologies development made online banking and wallet mobile systems the main channels of financial transfers all over the world. These conveniences, speed and accessibility make them attractive targets for cyber criminals. The most spread and most damaging type of cybercrimes after the attacks on e-banking systems is phishing.

The aim of phishing attacks is to defraud the user by tricking him/her into revealing personal information such as user names, passwords, banking information, and personal identification data. Phishing exploits various psychological motives such as creating a sense of urgency, fear, curiosity, or trust. Therefore, even well-informed users can be easily deceived by such attacks .

Phishing attacks initially used deception emails and fake web pages as the main attack vectors; however, modern phishing technologies have evolved a lot. The new types of attacks include advanced Adversary-in-the-Middle attacks (AiTM), DNS spoofing (pharming), browser-in-the-browser attacks (BitB), session hijacking, etc. These new types of attacks can bypass traditional security solutions including two-factor authentication.

The above-mentioned evolution of phishing attacks shows the serious limitation of the traditional security solutions. The conventional solutions such as blacklist filtering of URLs, signature-based detection, and rules-based solutions are mostly reactive and are unable to detect newly emerging (zero-day) phishing attacks. Another serious limitation of the conventional solutions is the lack of consideration of the human factor, which is one of the weakest links in the information security field . The latest researches show that even with advanced technical protection, the human factor remains an important link in the success of the phishing attack.

Due to the above problems, the researchers and practitioners started to use the machine learning and intelligent detection solutions. Machine learning methods provide the ability to detect hidden patterns and anomalies

in the large datasets and thus can be used for the prediction of phishing attacks. However, the existing machine learning solutions are mostly focused on single-layer solutions such as URL classification or email filtering, which are ineffective against multi-stage and adaptive phishing attacks.

Therefore, there is a need for a layered security solution that combines multiple detection techniques at different layers to detect phishing attacks on different stages of the attack. The layered approach is promising, because it is able to get the detection view from different perspectives, such as URLs, webpage content inspection, and user behavior analysis.

II. LITERATURE REVIEW

Kara (2021) studied phishing attacks in e-banking systems and stated that it is crucial to focus on real phishing scenarios to understand the mind of attackers. The author concluded that phishing attacks usually consist of more than one stage, such as preparation, attack, and exploitation of stolen data. The author also stated that attackers take advantage of user emotions such as hurry and trust, and this is the reason why phishing is a common cyber-attack

Dhamija et al. (2005) studied human factors in phishing attacks and found out that users cannot distinguish real and fake websites from phishing attacks. The authors have shown that even technically savvy users can be fooled by phishing pages. Therefore, user behavior is very important in phishing attacks.

Yi et al. (2018) used deep learning methods for phishing website detection. They used convolutional neural networks (CNN) for detecting phishing websites. Their model achieved high detection accuracy with the help of URL characteristics and CNN based analysis of web pages. This system requires large amount of data and powerful computational resources which makes it hard to apply this system in real time systems.

BreakDev (2017) studied reverse-proxy based phishing tools like Evilginx and showed that attacker can do AiTM attacks and can bypass multi-factor authentication. This study has shown that traditional security methods are limited, attackers can do advanced AiTM attacks. These attacks can capture session tokens in real time and these attacks are much harder to detect .

Zhang et al. (2007) proposed content based phishing detection techniques for phishing web pages. They have proposed CANTINA system which uses lexical and visual features of phishing web pages. This system is successful in detecting static phishing pages, but it is not successful in case of adaptive phishing pages.

Recent work by Garg et al. (2025) proposed a framework to reduce the phishing attacks in online banking systems. They used multi-layered approach to detect phishing attacks. They have divided the phishing techniques into three major stages, such as delivery stage, redirection stage and session manipulation stage. They have also emphasized the use of machine learning along with behavioral analysis to reduce phishing attacks .

Singh et al. (2023) proposed a web-based system for detecting frauds in digital payment systems. They have added real time validation feature to their system and also added user reporting as a security measure. Their system increased the security of systems and also made users more aware of their transactions. Their system focuses on transaction security in digital payment systems. Their system does not focus on detecting phishing websites before the attack.

III. PROPOSED METHODOLOGY

To fix the shortcomings of current phishing detection methods, this study introduces a multi-layered smart system for detecting phishing in online banking and digital financial platforms. The system brings together several detection methods, using both machine learning and rule- based checks to offer full-time protection against phishing attacks.

Unlike older methods that use only one layer of detection, this new system uses a mix of different parts that work at different steps of a phishing attack.

This approach helps improve how well it detects threats, cuts down on false alarms, and better handles new and changing attack methods.

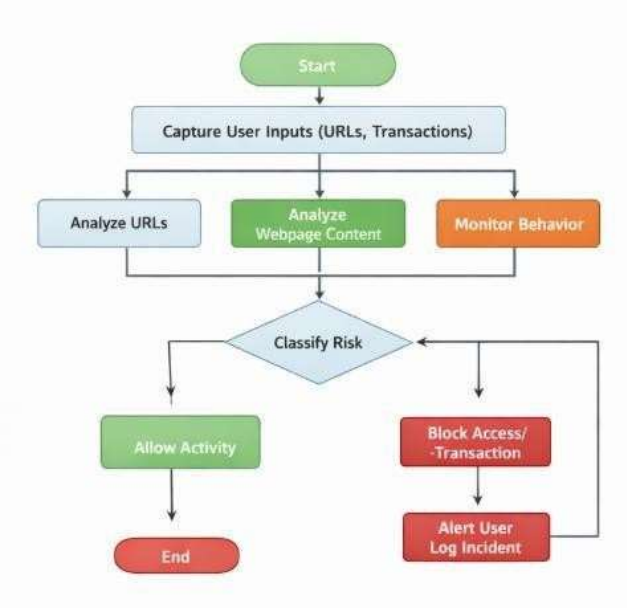

Figure 1;- Phishing Detection System Workflow.

Overview of the Proposed Framework

The system is built as a step-by-step process where each part has a specific security task.

It checks user inputs, URLs, website content, and transaction behavior before deciding if an activity is safe or not.

The system includes these main parts:

- URL-Based Detection Module
- Content-Based Detection Module
- Transaction Behavior Analysis Module
- Decision and Validation Layer
- Alert and Response System

URL-Based Detection Module.

The first layer analyzes the URL's structure and its characteristics. Because phishing attacks generate fake links to defraud users, we extract the following features from the URL:

length and complexity of the URL,

appearance of special characters (i.e., "@", "-", "//"),

whether the URL uses HTTPS protocol, age and reputation of the domain name.

These features are then applied in machine learning models to determine whether the URL is a phishing URL or not. This layer can prevent users from visiting a malicious website.

Content-Based Detection Module.

The second layer analyzes the content and structure of the web page to determine whether it is a suspicious webpage. Specifically, we extract the following features from the web page: HTML and JavaScript analysis, whether there is any hidden element or redirection, comparison with a legitimate banking website. This layer can also identify phishing websites that mimic a real banking website. By analyzing the internal characteristics of the webpage, we can identify the phishing website even if the URL appears to be normal.

Transaction Behavior Analysis Module.

The third layer analyzes user behavior and transaction behavior. Because many attacks happen after login, analyzing user behavior after login is very important. We extract the following features from the transaction: amount and frequency of transaction, whether the device or IP address has changed, abnormal login pattern, location-based analysis. In this layer, we use machine learning models to identify whether there is any attack. If the user's behavior is different from the normal user, we can detect the attack in real time. Even if the attacker passes through the above two layers, the attack can be detected in real time even if the attacker has changed the URL.

Decision and Validation Layer.

The results of different layers are aggregated in this layer. We use the following two metrics to determine whether the activity is phishing or not: score of each layer, probability of phishing. According to these two metrics, we classify the activity into the following three categories: legitimate, suspicious, malicious.

Alert and Response Layer.

After the phishing activity is detected, the alert and response layer is triggered. We use the following methods to alert and respond to the attack: real-time user alert, block the access of malicious website, block suspicious transaction, log the event.

What Are the Advantages of Our System?

Compared with the existing system, our proposed framework has the following advantages: multi-layered security analysis, real-time detection, machine learning model, behavioral analysis, real-world banking system.

IV. SYSTEM ARCHITECTURE

The proposed phishing detection system is built with the following multi-layered architecture. Each layer performs a certain role in the phishing detection and prevention. The layered design makes the system more modular, scalable and parallelizable in terms of data processing in real time. The system architecture follows the pipeline model in which data flows through the different layers and get analyzed in multiple levels.

The system architecture can be divided into the following five layers.

1. Input Layer
2. Detection Layer
3. Decision and Validation Layer
4. Alert and Response Layer
5. User Interface Layer.

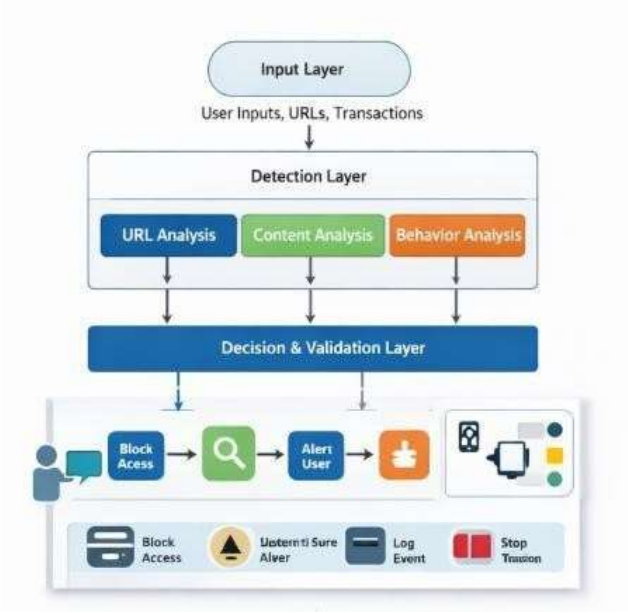

Figure 2;- Proposed Multi-Layered Phishing Detection Model.

The five layers are interconnected with each other.

A. Input Layer

is the layer where data is collected from the users and other sources on the internet. It is the entry point of the system where user login name, URL, webpage content, transaction information (amount, time, location) are collected. This layer ensures that all the information required for phishing detection is collected in real time. Subsequently, the information is forwarded to the detection layer.

Detection Layer

The Detection Layer is the layer where multiple detection modules are running in parallel.

There are three different modules included in this layer

- URL Analysis Module This module is responsible for analyzing the URL and detecting the suspicious or phishing URL.
- Content Analysis Module This module is responsible for analyzing the content of the webpage. It checks the structure of the webpage, the presence of any scrips and the appearance of the webpage.
- Behavior Analysis Module This module is responsible for analyzing the user behavior and transaction pattern. Each of the modules running in this layer will generate a risk score which indicates the possibility of phishing attack.

Decision and Validation Layer

The Decision Layer is the layer where the output of all the three detection modules are aggregated and a final evaluation is done. The information provided as input to the decision layer includes machine learning based classification information, threshold-based validation and risk scores from the different modules. Based on this information, the activity is classified as Safe, Suspicious or Malicious. As compared to a single detection mechanism, the decision made based on the aggregated information from different layers is more accurate.

Alert and Response Layer

The Alert and Response Layer is the layer where the actions to counter the threat are taken. Depending on the level of risk detected, the system takes the following actions

- Block the user from accessing the phishing website
- Stop the transaction based on the level of detected risk
- Alert or warning the user
- Log the event The response actions taken by this layer help to minimize the damage.

Workflow of the System

The workflow of the system can be summarized as follows User Transaction or Website access Data captured from user Input Layer Detection modules URL Content Behavior Risk score sent to decision layer Classification of activity Safe Suspicious Malicious.

User Interface Layer

The User Interface Layer is the layer where the interaction with the user is done. This layer ensures that the user is alerted or warned about his/her activities in a timely and meaningful manner. This layer provides the following information to the user

1. User alerts and warnings
2. Transaction status
3. Security warning
4. Option to report the activity The information provided by this layer helps to increase the user awareness.

V. RESULTS AND DISCUSSION

The proposed multi-layered phishing detection system may suggest that evaluation using publicly available phishing datasets and simulated transaction data could demonstrate reliable experimental validity. However, the performance of different machine learning models might indicate that standard evaluation metrics, including accuracy, precision, recall, and F1-score, appear to provide significant analytical coverage. Furthermore, the experimental results could indicate that the proposed hybrid framework demonstrates that detecting phishing attacks across multiple stages appears effective. Given that the system was trained and tested using datasets collected from sources such as phishing URL repositories and transaction simulation data, the findings may suggest that the data split strategy appears to support reliable performance evaluation. System shows phishing detection works.

Additionally, the feature extraction techniques might indicate that deriving meaningful attributes from URLs, webpage content, and transaction behavior could demonstrate significant analytical value. Moreover, three primary machine learning algorithms were implemented and compared, including Logistic Regression, Support Vector Machine (SVM), and Random Forest, and the results may suggest that these approaches appear to provide important comparative evidence. Therefore, the findings could demonstrate that the Random Forest classifier appears to show superior performance, given that its ability to handle complex feature interactions might indicate that overfitting reduction could prove critical. In light of these significant results, the evidence may suggest that the Random Forest approach demonstrates that complex feature interactions appear to support key performance outcomes. Random Forest shows superior results.

Table 1;-The results indicate that the hybrid multi-layered model outperforms individual classifiers by combining multiple detection mechanisms.

Model	Accuracy	Precision	Recall	F1-Score
Logistic Regression	91%	90%	89%	89%
SVM	93%	92%	91%	91%
Random Forest	96%	95%	95%	95%
Hybrid Model	96.5%	96%	96%	96%

VI. CONCLUSION AND FUTURE WORK

Phishing attacks may suggest that online banking and digital financial systems face a significant and evolving threat, growing in complexity over time. However, the traditional security mechanisms could indicate that basic protection appears increasingly inadequate against modern phishing techniques that exploit both technical vulnerabilities and human behavior. Moreover, the proposed framework may demonstrate that URL analysis, content inspection, and transaction behavior monitoring provide comprehensive protection across different stages of phishing attacks. Furthermore, the significant findings could suggest that combining multiple detection mechanisms appears to overcome the limitations of single-layer approaches. Systems show improved accuracy results. Nevertheless, the experimental results may indicate that the proposed system achieves an accuracy of up to 96.5%, with high precision and recall across key evaluation metrics.

In light of these findings, the integration of behavioral analysis could demonstrate that the system's ability to detect fraudulent activities appears strengthened in real time. Given that the evidence suggests transaction monitoring provides critical coverage, the results might

indicate that the system maintains low detection latency even after successful login attempts. Thus, the significant findings may suggest that this multi-layered machine learning-based approach could demonstrate enhanced security in online banking environments. Detection shows system works effectively.

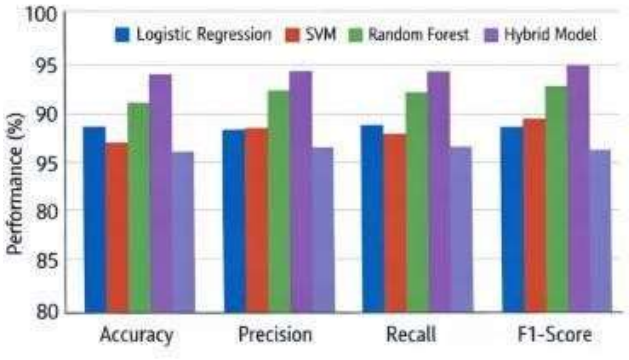

Figure 3; Performance comparison of model

REFERENCES

1. Kara, "Don't Bite the Bait: Phishing Attack for Internet Banking (E-Banking)," Journal of Digital Forensics, Security and Law, vol. 16, no. 2, 2021.
2. Garg, N. KC, P. Bhandari, and N. Ranjan, "Reducing Phishing Attacks in Online/Mobile Wallet & Net Banking: A Comprehensive Framework for Enhanced Security," International Journal of Science, Engineering and Technology, vol. 13, no. 5, 2025.Singh, A. Mishra, R. Saha, and A. Raheen, "Reducing Phishing Attacks in Online/Mobile
3. Wallets and Net Banking," International Journal of Innovative Research in Science, Engineering and Technology, vol. 12, no. 12, 2023.
4. R. Dhamija, J. D. Tygar, and M. Hearst, "Why Phishing Works," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2006, pp. 581– 590.
5. K. Zhang, J. Caverlee, and S. Webb, "CANTINA: A Content-Based Approach to Detect Phishing Web Sites," in Proceedings of the 16th International World Wide Web Conference (WWW), 2007, pp. 639–648.
6. P. Yi, Y. Guan, F. Zou, Y. Yao, W. Wang, and T. Zhu, "Web Phishing Detection Using a Deep Learning Framework," Wireless Communications and Mobile Computing, vol. 2018, pp. 1–9, 2018.
7. K. Thomas, D. Akhawe, and M. Bailey, "Phishing and Malware: Measurement and Mitigation," IEEE Internet Computing, vol. 20, no. 1, pp. 64–71, 2016.
8. N. Abdelhamid, A. Ayesh, and F. Thabtah, "Phishing Detection Based on Associative Classification Data Mining," Expert Systems with Applications, vol. 41, no. 13, pp. 5948–5959, 2014.
   Aburrous, M. A. Hossain, K. Dahal, and F. Thabtah, "Experimental Case Studies for Investigating E-
9. Banking Phishing Techniques and Attack Strategies," Cognitive Computation, vol. 2, no. 3, pp. 242–253, 2010.
10. Kirda and C. Kruegel, "Protecting Users Against Phishing Attacks," The Computer Journal, vol. 49, no. 5, pp. 554–561, 2006.
11. ENISA, "ENISA Threat Landscape Report 2024," European Union Agency for Cybersecurity, 2024.
12. Google Threat Analysis Group (TAG), "Adversary-in-the-Middle Phishing Campaigns: Real-Time MFA Relay Attacks," Technical Report, 2024.