International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 03, March 2026)

PhishGuard – Real Time Phishing Link Detection

Deokar V.S[1], M. R. Shaikh[2], Deokar Shraddha[3], Bidve Sujal[4], Gorade Chetan[5], Daghale Pranjal[6]

[1,2]*Lecturer, Department of Computer Technology, Sanjivani K.B.P Polytechnic, Kopargaon, India*
[3,4,5,6]*Research Scholar, Department of Computer Technology, Sanjivani K.B.P Polytechnic, Kopargaon, India*

***Abstract*-- Due to the increased rate of growth of internet usage and online service availability, the risk of cyber attacks has increased, and one of the most common cyber attacks is phishing, which tries to collect sensitive information such as login credentials, bank details, and other personal information from the victim. Phishing attacks are often carried out through harmful URLs delivered through emails, social media, and messaging platforms, making it difficult for the victim to recognize the attack before they click on the link. Although several security solutions are available, they are often complicated, slow, and not easily accessible for the general public. To solve this problem, this paper proposes a real-time phishing link detection system called PhishGuard, which increases user security by detecting suspicious URLs before the victim clicks on the link. This security system uses artificial intelligence for URL analysis and incorporates a mobile app interface using modern mobile app development technologies. It analyzes different aspects of URLs, such as domain name, suspicious patterns, and safety, and tries to understand whether it is safe or harmful for the victim. By using React Native for mobile app development, this security system is capable of providing instant security and ease of use for the general public, increasing the safety of internet usage for all users.**

***Keywords*--Phishing Detection, Artificial Intelligence, URL Analysis, Cyber Security, Real-Time Security System, Mobile Application Framework.**

I. Introduction

The increasing rate of internet usage and services has led to a rise in cyber attacks, especially phishing attacks. These types of cyber attacks are often in the form of suspicious emails, websites, or suspicious links shared through various messaging services or social media sites. These types of cyber attacks often result in the theft of sensitive information, financial loss, or unauthorized access to personal or organizational accounts. Even though the importance of internet security has become a major topic of awareness, the sophistication of phishing attacks has made it difficult for internet users to identify suspicious or harmful links.

In order to overcome this problem, this research aims to develop a phishing link detection system named PhishGuard. This system will be used to identify suspicious or harmful internet links before visiting the sites. The proposed system will be developed using AI-based URL analysis along with a mobile application.

This project will be focused on designing the system architecture, developing a mobile application, and implementing the phishing detection algorithms. The proposed solution will be useful for internet users to remain alert while using the internet.

II. Literature Survey

Literature survey reveals that phishing detection systems are very important for protecting people from cyber crimes. They help detect harmful URLs and fake websites. Various research works have been done on different approaches for detecting phishing attacks. Some of the approaches are using blacklist databases, using heuristics, and using Artificial Intelligence-based detection methods. These approaches check URLs, domain names, and webpage characteristics and try to determine whether the link is genuine or not. Literature survey in the area of cybersecurity has emphasized the importance of secure data handling, effective threat detection, and response systems for reducing the possibility of cyber attacks.

Mobile security applications have been designed for providing users with useful tools for detecting phishing attacks on their mobile phones. Real-time detection systems help raise the level of awareness for mobile device users, who are notified about suspicious links before visiting potentially harmful websites. Moreover, the utilization of Artificial Intelligence and automated analysis techniques has enhanced the accuracy of phishing detection systems.

However, existing solutions may cover only limited aspects of phishing detection. They may include extensions, email filtering solutions, or static blacklists. These solutions may not cover newly created phishing links or may not provide a user-friendly interface for regular users. Therefore, there is a need for a practical, user-friendly solution that includes link analysis, intelligent detection capabilities, and mobility within one security solution.

III. Proposed Solution

In order to overcome the limitations of the existing phishing detection systems, the proposed PhishGuard system has been designed to introduce an intelligent solution that is user-friendly in detecting phishing links quickly. This is achieved by analyzing the suspicious URLs using automated techniques.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 03, March 2026)

The proposed PhishGuard system, presents a solution for the detection of phishing links using intelligent techniques by analyzing various attributes of the URL. The system will be capable of analyzing the features of the URL, including the length of the URL, the structure of the domain, the presence of suspicious keywords, and the security features of the URL, including the HTTPS protocol. The proposed system will differ from the existing system in that it will not depend on the blacklist approach; rather, the system will perform real-time analysis of the URL, enabling the user to input the suspicious URL in the system and obtain the result immediately regarding the safety of the URL or the presence of phishing.manner.

In addition to accurate detection, PhishGuard is designed as a user-friendly mobile application that can be easily used by both technical and non-technical users. The simple interface allows users to quickly verify links and receive clear alerts if a phishing threat is detected. The system also promotes cybersecurity awareness by providing warning messages and explanations about unsafe links. By combining intelligent URL analysis, real-time detection, and an accessible mobile platform, PhishGuard helps protect users from phishing attacks and supports safer online browsing.

Table 1
Focus & Scope of the Proposed System

Focus	Scope
Mobile Cybersecurity Application Development	Android-based application for detecting phishing threats in real time
Phishing Detection Using Artificial Intelligence	AI model analyzes URLs, messages, and login pages to detect phishing patterns
Real-Time Threat Monitoring	Continuous scanning of suspicious links, emails, and login attempts
Secure User Authentication	Firebase Authentication for safe login and user management
Cloud-Based Data Storage	Firebase Firestore for storing user data, reports, and detection logs
Mobile Security Infrastructure	Scalable system architecture for future integration with browsers and messaging apps

IV. Research & Review

A detailed research and review process was conducted during the development of the **PhishGuard** system to understand the growing problem of phishing attacks and the existing solutions used to detect them. The research focused on common phishing techniques used by attackers, such as malicious URLs, fake websites, and deceptive links shared through emails, social media platforms, and messaging applications. It was observed that many internet users still click on suspicious links because they lack proper detection tools and awareness about phishing threats. This often leads to serious consequences such as data theft, financial loss, and unauthorized access to personal information.

The review of existing phishing detection systems showed that many current solutions rely on browser extensions or databases of known malicious URLs, which are often unable to detect newly created phishing links quickly. This highlighted the need for a more efficient and real-time detection approach that is also easy for everyday users to access. As a result, a mobile-based phishing detection platform was proposed to allow users to verify suspicious links quickly and conveniently. This research ultimately led to the development of the **PhishGuard** system, which aims to enhance online safety and reduce the risks of phishing attacks.

V. Methodology

PhishGuard was developed following a structured and requirement-driven development process. The development was initiated by conducting a thorough analysis of the prevalent methods of phishing and the tools used for the purpose, in order to understand the gaps that the current tools are facing. Based on the analysis, the major requirements for the system were formulated, including the need for a tool that can perform a real-time analysis of the URLs, the need for intelligent tools, the need for a user-friendly mobile-based application, and the need for a tool that can quickly alert the users about harmful links.

It utilizes a client-server architecture, which helps in efficient processing and communication between the mobile application and detection backend. The mobile application was developed using React Native, allowing for multiple platforms and user interaction. Upon entering a URL, the system analyzes various features, including URL length, domain composition, suspicious keywords, and usage of secure protocols like HTTPS. By analyzing these attributes, the system categorizes each URL as either phishing or legitimate, providing feedback to the user.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 03, March 2026)

VI. System Architecture

The **system architecture of PhishGuard** follows a client–server model. The mobile application (built with React Native) acts as the **frontend layer**, where users interact with the system by submitting URLs, messages, or suspicious links for analysis. The app sends this data to the backend through secure API calls. The frontend is responsible for user authentication, displaying analysis results, and providing a simple interface for reporting or checking phishing attempts.

The **backend layer** processes the received data using phishing detection logic and integrates with cloud services such as Firebase for authentication, database storage, and file management. The backend analyzes the submitted URLs or messages using predefined rules or machine-learning models to determine whether they are safe or potentially malicious. After processing, the results are sent back to the mobile app, where users can view warnings, risk levels, and safety recommendations, ensuring quick and reliable phishing detection.

VII. Flow Of PhishGuard

The working flow of **PhishGuard** begins when a user opens the app and logs in or signs up using secure authentication provided by **Firebase Authentication**. After logging in, the user can enter or paste a suspicious URL, message, or link into the input field for analysis. The app sends this data from the mobile interface (built with **React Native**) to the backend service through an API request. This ensures the user input is securely transmitted for further inspection.

Once the data reaches the backend, the system checks the link or content using phishing detection logic and compares it with stored patterns or security rules in the database. The results are processed and stored using cloud services like **Firebase Firestore**. After analysis, the backend sends a response back to the app indicating whether the link is **safe, suspicious, or phishing**. The mobile app then displays the result to the user along with warnings or safety recommendations, helping them avoid potential phishing attacks and improving overall online security.For the Admin role, users possess more advanced privileges. Admins can create, edit, or manage events, access all student registrations, and send announcements. Their operations are

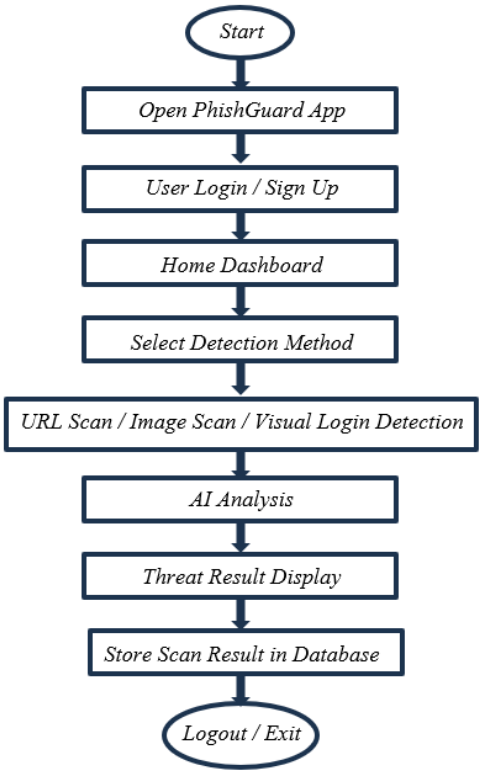

Fig1: PhishGuard -Flowchart with Process-Flow

Table 2
Performance Evaluation of One Platform

Parameter	Result	Remark
Authentication System	Successful	Enrolment-based login
Email Verification	Functional	Secure account validation
Role-Based Access	Accurate	Student/Admin separation
Event Creation	Operational	Admin-controlled
Event Registration	Real-time	Instant Firestore update
Database Security	Enforced	Firestore rules applied
System Stability	Stable	No crash during testing

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 03, March 2026)

VIII. Future Scope

In the future, **PhishGuard** can implement an **automatic background scanning feature** that continuously monitors incoming links and messages without requiring manual input from the user. The app can run a lightweight background service that scans URLs from SMS, notifications, or copied links and instantly checks them against phishing detection rules and databases. If a suspicious or malicious link is detected, the system can immediately notify the user with a warning alert, helping them avoid opening harmful websites.

IX. Conclusion

PhishGuard is a phishing link detector that works in real time and is aimed at standing up to the increase in phishing URLs and the fact that people still underestimate the risks of such URLs. Its objective is simple, and that is to provide users with a clear and effective way to check suspicious URLs before they click on them. It works by checking the various characteristics of the link and raising alarm flags to prevent people from being victims of phishing. It works through a secure authentication system, cloud database, and real-time alerts to create a centralized digital academic space.

The above design shows that a clean client-server architecture and the use of intelligent URL analysis can create a fast and reliable phishing detection system. It works by allowing the user to quickly scan any link they are not sure about through the mobile app. The analysis module, meanwhile, works by considering the characteristics of the link, such as the structure of the domain, the length of the URL, questionable words, and the use of HTTPS.

Overall, PhishGuard is a practical and user-friendly cybersecurity tool for real-time phishing detection. From the research, it is clear that the creation of the PhishGuard system has the potential to increase users' cybersecurity awareness significantly and prevent them from accessing malicious websites. It is, therefore, a system that works to create a better cybersecurity environment by providing users with an efficient and reliable phishing detection system.

Acknowledgment

The authors would like to thank the Department of Computer Engineering of our institution for providing the necessary academic environment, technical resources, and infrastructure required for the successful development of PhishGuard.

We are deeply thankful to our project guide and faculty mentors for their continuous supervision, expert guidance, and constructive suggestions throughout the research, design, and implementation process. Their valuable inputs on system architecture, security mechanisms, and cloud integration have played an important role in improving the quality and reliability of the proposed system.

We also appreciate the college administration and staff members who have provided important inputs on existing academic workflows and institutional requirements. Their practical inputs have helped in aligning the system design with real-world requirements.

Special thanks are given to our peers and fellow students who have participated in testing and provided meaningful inputs during the evaluation phase. Their inputs have played an important role in improving usability, interface clarity, and functional performance.

Finally, we acknowledge all individuals who have directly or indirectly supported us during this project and contributed to the successful completion of this research work.

REFERENCES

[1] Christopher D. Manning, Prabhakar Raghavan, & Hinrich Schütze (2008). Introduction to Information Retrieval. Cambridge University Press.

[2] Ian Goodfellow, Yoshua Bengio, & Aaron Courville (2016). *Deep Learning.* MIT Press.

[3] IEEE Xplore Digital Library. Research papers on Phishing Detection Systems, Cybersecurity Applications, and Machine Learning for Threat Detection. Available at: https://ieeexplore.ieee.org.

[4] ResearchGate. (2020–2024). Research papers on Phishing Website Detection, URL Analysis, and AI-based Cybersecurity Systems. Available at: https://www.researchgate.net.

[5] Google Developers. AI and Machine Learning APIs for mobile security applications. Available at: https://developers.google.com