JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

PhishShield – A Web & Mobile Application for Phishing URL Detection

ANANYA LIMAN, AYUSH WALHEKAR, PARTH BARGE, ATHARVA LANDGE
STUDENT
RASIKLAL M DHARIWAL INSTITUTE OF TECHNOLOGY CHINCHWAD

Abstract- PhishShield is a web and mobile application designed to detect and prevent phishing attacks by identifying malicious URLs in real time. The system analyzes website links using advanced machine learning algorithms, blacklist databases, and heuristic techniques to determine their authenticity. It helps users verify suspicious links received through emails, messages, or social media before accessing them, thereby reducing the risk of data theft and cyber fraud. PhishShield provides instant alerts, detailed risk reports, and user-friendly guidance to promote safe browsing habits. The application supports both individual users and organizations by offering secure access across multiple platforms. With an intuitive interface and fast detection mechanism, PhishShield ensures reliability and ease of use. By enhancing digital security awareness and minimizing online threats, PhishShield aims to create a safer internet environment and protect users from evolving phishing attacks in today's interconnected digital world.

1. **Index Term-** Phishing Detection, Cyber Security, Malicious URLs, Machine Learning, Web and Mobile Application

I. INTRODUCTION

The increasing use of digital platforms and online communication has led to a rapid rise in phishing attacks, posing serious threats to users' personal and financial information. Many existing security systems lack real-time detection, accuracy, and user-friendly interfaces, making them difficult for common users to rely on. The absence of centralized monitoring and limited awareness among users further increases the risk of falling victim to fraudulent links. Manual verification methods are time-consuming and unreliable, often failing to detect advanced phishing techniques. These challenges significantly affect online safety and emphasize the need for a modern, intelligent, and comprehensive solution for phishing detection.

The purpose of the proposed PhishShield system is to enhance cybersecurity by providing an automated and centralized platform for detecting malicious URLs. It aims to ensure accurate, fast, and reliable identification of phishing websites using advanced algorithms and machine learning techniques. The system also focuses on creating a structured database of verified and harmful links, improving transparency and digital trust.

At PhishShield, we are committed to strengthening online security through innovative, reliable, and accessible digital solutions. Our mission is to protect users from cyber threats by delivering safe browsing experiences, promoting awareness, and supporting secure online practices.

PhishShield is designed as an integrated platform that supports both web and mobile environments. This approach enables continuous monitoring, real-time threat detection, and quick response to evolving cyber risks, ensuring enhanced protection and confidence for users in the digital world.

Furthermore, PhishShield emphasizes user education and awareness as a key component of cybersecurity. The system provides informative alerts, safety tips, and detailed reports to help users understand potential threats and improve their online behavior. By combining advanced technology with user-centric design, PhishShield empowers individuals and organizations to actively participate in protecting their digital identity and maintaining a secure online presence.

II. LITERATURE REVIEW

1.**Research Existing Applications:** Several web and mobile-based cybersecurity applications have been developed to detect phishing websites and malicious URLs. These systems mainly focus on blacklist-based detection, machine learning models, and browser extensions. Studying their features, architecture, and performance helps in understanding current industry standards and limitations.
2.Review Academic Papers: Various research papers have discussed phishing detection using data mining, artificial intelligence, and machine learning techniques. These studies highlight methods such as URL feature extraction, neural networks, and classification algorithms. Key findings emphasize the importance of accuracy, speed, and adaptability in detecting evolving phishing attacks.
3.Explore Development Frameworks and Tools: Modern phishing detection systems commonly use frameworks for web and mobile development, along with libraries for machine learning and data analysis. Evaluating these tools helps in selecting suitable technologies for implementing secure and scalable applications.
4.Study Best Practices: Best practices include designing user-friendly interfaces, ensuring real-time detection, maintaining updated databases, and implementing strong encryption techniques. These practices improve system reliability and user trust.
5.Consider Security and Privacy Standards: Data protection laws and cybersecurity standards emphasize secure data handling, user privacy, and encrypted communication. Compliance with these standards is essential for building trustworthy applications.
6.Compare Different Detection Approaches: Literature compares blacklist-based, heuristic-based, and machine learning-based methods. Each approach has advantages and limitations, guiding the selection of an effective hybrid detection model.
7.Identify Challenges and Solutions: Common challenges include high false detection rates, evolving phishing techniques, and performance issues. Researchers propose adaptive learning models and continuous system updates as solutions.
8.Document Research Findings: The reviewed studies provide valuable insights into detection methods, system design, and security strategies. These findings help in shaping the architecture and implementation of the PhishShield application for improved accuracy and user safety.
9.Analyze User Behavior and Awareness: Several studies focus on user behavior, awareness levels, and response patterns toward phishing attacks. Understanding human factors helps in designing better alert systems, educational modules, and user guidance features within the application.
10.Evaluate System Performance and Scalability: Research also emphasizes evaluating system performance in terms of detection speed, accuracy, and scalability. These studies highlight the importance of optimizing system resources to handle large volumes of URL data efficiently while maintaining high reliability.

III. Scope of the website

The theoretical scope of the PhishShield website and mobile application encompasses the development of a comprehensive digital platform designed to enhance online security and protect users from phishing attacks. The system is intended to serve as a centralized hub for verifying suspicious URLs, providing real-time threat analysis, and offering cybersecurity awareness resources to individuals and organizations. It aims to support a wide range of users, including students, professionals, businesses, and general internet users, by ensuring safe and reliable browsing experiences.
Functionally, the platform includes features such as URL scanning, instant risk alerts, detailed threat reports, user feedback systems, and secure account management. These components are integrated within a user-friendly, responsive, and accessible interface suitable for both web and mobile environments. Technologically, the system is built using modern development tools, machine learning models, and secure communication protocols to ensure accuracy, privacy, and scalability.
The platform also holds future potential for expansion into browser extensions, enterprise-level security solutions, multilingual support, and advanced threat intelligence integration. In essence, PhishShield aims to bridge the gap between cybersecurity technology and everyday internet usage by providing an informative, interactive, and reliable digital protection system.

IV. Requirement analysis - Functional requirements, performance requirements, security requirements etc

Function Requirement:

- The system should allow users to register and log in securely through web and mobile platforms. Users should be able to manage their profiles, update personal information, and change passwords.
- The system should enable users to scan and verify suspicious URLs in real time. It should analyze links using detection algorithms and classify them as safe, suspicious, or malicious.
- The application should maintain a centralized database of phishing and legitimate URLs. Administrators should be able to update, manage, and monitor this database regularly.

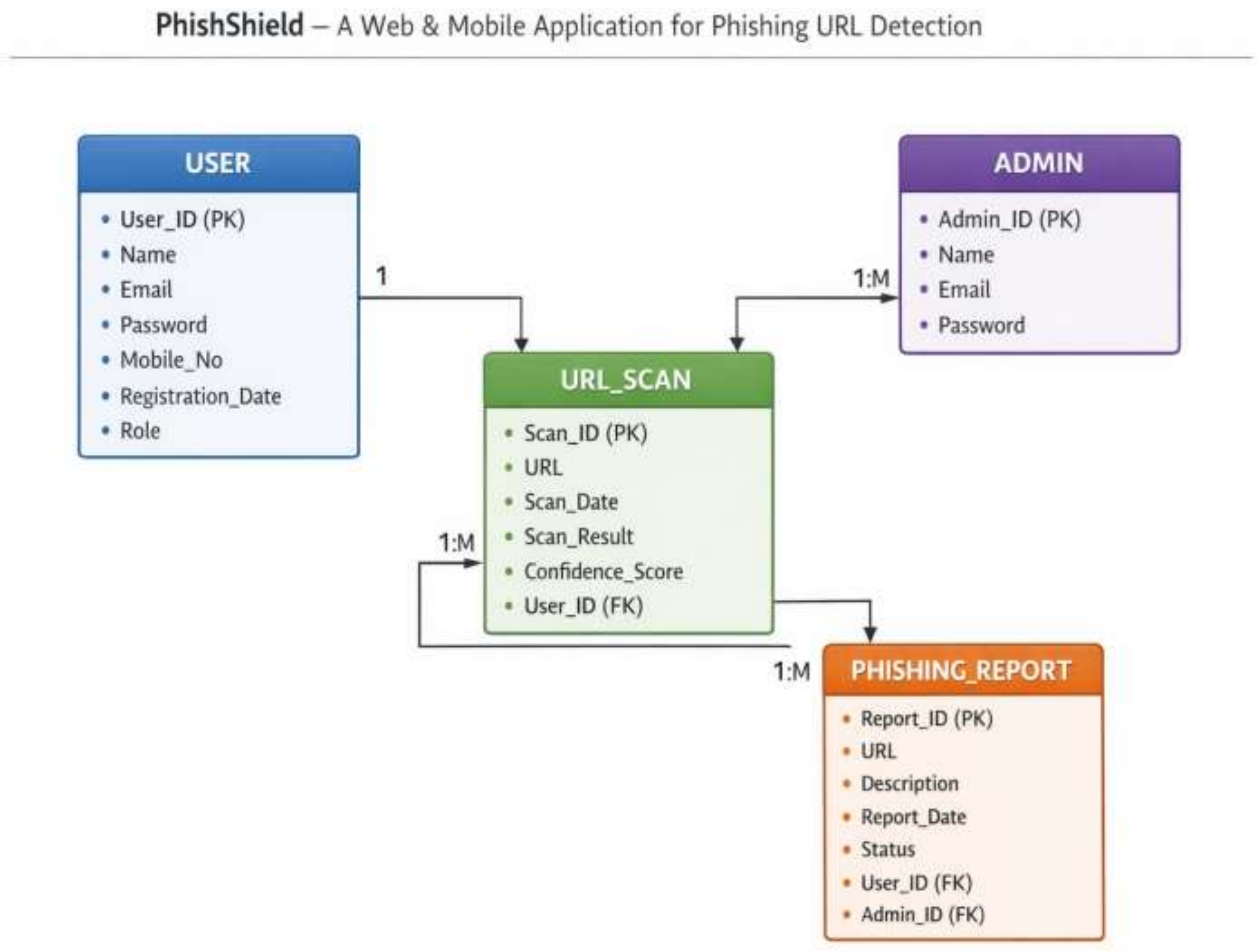
- Users should be able to submit suspicious links for analysis and receive instant alerts and detailed risk reports.
- The system should generate reports on detected threats, user activities, and security trends to support monitoring and analysis.
- The system should provide educational resources, safety tips, and notifications to improve user awareness about phishing attacks.

Non-Functional Requirement:

- The system should be highly responsive and provide real-time URL analysis with minimal delay.
- The application should be available 24/7 with minimal downtime for maintenance and updates.
- The system should use strong encryption techniques to secure user data, scanned URLs, and communication channels.
- The application should ensure high accuracy and reliability in phishing detection with low false-positive rates.
- The system should comply with cybersecurity standards and data privacy regulations to protect user information.
- The platform should be scalable to support a growing number of users and increasing volumes of URL analysis.

V. Entity Relationship Diagram (ERD):

The Entity Relationship (ER) model defines the conceptual structure of the PhishShield system database. It represents real-world entities involved in phishing detection and their relationships with one another. At the design level, the ER model serves as an effective tool for organizing data and ensuring logical consistency within the system. It helps in visualizing how different components of the application interact and how information is stored and managed. An entity represents a real-world object that is identifiable and relevant to the system. In PhishShield, entities include users, URLs, detection reports, feedback records, and administrators. Each entity contains specific attributes that describe its characteristics. For example, a user entity may include user ID, name, email, password, and role, while a URL entity may include URL ID, link address, detection status, and scan date. All attributes hold specific values that define the identity of each entity. These attributes enable efficient storage, retrieval, and management of data within the system. The relationships among entities define how users interact with URLs, how reports are generated, and how administrators manage system activities. This ER diagram is associated with the overall functioning of the PhishShield platform, illustrating how different users perform various operations based on their assigned roles. It helps in understanding system workflows and ensures smooth coordination between data entities in the phishing detection process.


PhishShield – A Web & Mobile Application for Phishing URL Detection
USER
User_ID (PK)
Name
Email
Password
Mobile_No
Registration_Date
Role
1
ADMIN
Admin_ID (PK)
Name
Email
Password
1:M
URL_SCAN
Scan_ID (PK)
URL
Scan_Date
Scan_Result
Confidence_Score
User_ID (FK)
1:M
1:M
PHISHING_REPORT
Report_ID (PK)
URL
Description
Report_Date
Status
User_ID (FK)
Admin_ID (FK)

VI. Conclusion

In conclusion, PhishShield represents a forward-thinking, secure, and innovation-driven solution for modern digital safety. With a strong focus on advanced phishing detection techniques, real-time analysis, and user awareness, the system is well-positioned to address the growing challenges of online fraud and cybercrime. By integrating intelligent algorithms with user-friendly design, PhishShield aims to provide reliable and accessible protection for users across web and mobile platforms. The application emphasizes accuracy, speed, and continuous system updates to effectively respond to evolving phishing threats. A modern and intuitive interface empowers users to easily verify suspicious links and make informed online decisions. Regular updates ensure that the system remains effective against new attack patterns and emerging risks. By promoting safe browsing practices, maintaining high security standards, and enhancing cybersecurity awareness, PhishShield contributes to building a safer digital environment. As the platform continues to evolve, its focus on scalability, regulatory compliance, and technological advancement ensures long-term reliability, user trust, and success in protecting users from phishing attacks in both personal and professional digital spaces.

VII. References

1. www.google.com
2. www.youtube.com
3. www.cybersecurity.gov
4. **Phishing and Countermeasures** by Markus Jakobsson and Steven Myers – Explains phishing techniques and defense mechanisms.
5. **Machine Learning for Cybersecurity** by Jason Brownlee – Covers machine learning applications in security systems.
6. **Web Security for Developers** by Malcolm McDonald – Focuses on building secure web applications.
7. **Practical Malware Analysis** by Michael Sikorski and Andrew Honig – Discusses malware and phishing-related threats.
8. **Cybersecurity and Cyberwar** by P.W. Singer and Allan Friedman – Explains modern cybersecurity challenges.
9. **The Art of Invisibility** by Kevin Mitnick – Provides insights into online privacy and digital security practices.