IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, February 2026
Impact Factor: 8.2

Design and Implementation of a Web-Based Intelligent Scam and Phishing Detection System Using Rule-Driven Risk Scoring

Asiya S. Khan[1], Monika G. Manapure[2], Prof. Rahul Lilhare[3]
Department of Computer Application[1,2,3]
KDK College of Engineering, Nagpur, India
asiyaskhan.mca24f@kdkce.edu.in, monikagmanapure.mca24f@kdkce.edu.in, rahul.lilhare@kdkce.edu.in

Abstract: *The rapid expansion of digital communication platforms has led to a significant increase in scam and phishing attacks. Cybercriminals use deceptive messages, fraudulent links, and social engineering strategies to exploit users and extract sensitive information. This paper presents the design and implementation of a web-based intelligent scam and phishing detection system developed using Python for backend processing and HTML, CSS, and Bootstrap for frontend development. The proposed system employs a rule-driven risk scoring mechanism combined with logical inference techniques to analyze user-input messages and detect potential threats. Suspicious indicators such as sensitive keywords, urgency triggers, and shortened URLs are evaluated to compute a cumulative risk score. Based on this score, the system classifies content as Safe, Suspicious, or Scam. The system also provides reason generation, scam category identification, safety recommendations, encrypted data storage, and historical record management. The implemented solution enhances cybersecurity awareness and assists in proactive fraud prevention.*

Keywords: Scam Detection, Phishing Detection, Risk Scoring System, Rule-Based Detection, Cyber Security, Web Application

I. INTRODUCTION

The rapid growth of digital communication and online financial services has significantly increased the risk of cyber fraud activities. Among these threats, scam and phishing attacks are the most common and harmful forms of cybercrime. These attacks aim to deceive users into revealing sensitive information such as passwords, banking credentials, one-time passwords (OTP), and personal data. Fraudulent emails, messages, and websites often imitate legitimate organizations to gain user trust and manipulate victims. Phishing messages commonly use psychological techniques such as urgency, fear, rewards, and authority-based manipulation. Examples include fake bank alerts, lottery winnings, job offers requiring payment, and investment schemes promising unrealistic profits. With the widespread use of social media platforms and online banking systems, the frequency and sophistication of such attacks have increased substantially. Many users are unable to identify subtle warning signs such as suspicious URLs, shortened links, or high-risk keywords.Traditional spam filters and manual verification methods are often insufficient to detect modern phishing attempts. Therefore, there is a need for an intelligent and systematic approach to analyze suspicious content and assess its risk level effectively. While machine learning-based detection systems provide high accuracy, they require large datasets and complex training processes. In contrast, rule-driven logical systems offer transparency, lower computational requirements, and clear reasoning for detection decisions.This paper presents the design and implementation of a web-based intelligent scam and phishing detection system developed using Python for backend processing and HTML, CSS, and Bootstrap for frontend design. The proposed system employs a rule-driven risk scoring mechanism that evaluates suspicious indicators such as sensitive keywords, urgency triggers, and suspicious links. Based on the calculated risk score, the system classifies

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, February 2026
Impact Factor: 8.2

messages into Safe, Suspicious, or Scam categories. Additionally, it provides reason generation, scam categorization, safety suggestions, encrypted storage, and history management features to enhance user awareness and cybersecurity protection.

II. LITERATURE REVIEW

The increasing prevalence of phishing and scam attacks has motivated extensive research in the field of cybersecurity. Various approaches have been proposed to detect fraudulent messages, malicious URLs, and deceptive communication patterns. Existing detection techniques can broadly be categorized into machine learning-based methods, heuristic-based systems, and rule-driven detection mechanisms.Several researchers have implemented machine learning algorithms such as Logistic Regression, Support Vector Machines (SVM), Naïve Bayes, and Random Forest classifiers for phishing detection. These approaches analyze large datasets containing labeled phishing and legitimate samples to train predictive models. Studies have shown that machine learning models can achieve high detection accuracy when trained with sufficient and quality data. However, such models require continuous retraining, feature engineering, and computational resources, which may increase system complexity.Other research has focused on URL-based detection techniques, where domain characteristics, URL length, presence of special characters, and shortened links are analyzed to determine suspicious behavior. Additionally, some systems incorporate Natural Language Processing (NLP) techniques to evaluate textual content and detect deceptive language patterns commonly used in scam messages.Heuristic and rule-based systems have also been explored as lightweight alternatives. These systems rely on predefined logical rules and pattern matching to identify suspicious indicators such as sensitive keywords (e.g., “OTP,” “urgent,” “lottery”), unusual hyperlinks, and abnormal request patterns. Although rule-based approaches may not adapt automatically like machine learning models, they offer transparency in decision-making and provide clear explanations for detection results. This interpretability enhances user trust and system reliability.Recent studies emphasize the importance of combining detection mechanisms with user awareness features such as risk scoring, reason explanation, scam categorization, and preventive guidance. Such integrated systems not only identify threats but also educate users about potential risks.Based on the analysis of existing research, it is evident that there is a need for an efficient, interpretable, and web-accessible detection system that balances performance and simplicity. The proposed system in this paper adopts a rule-driven risk scoring methodology integrated within a web-based platform to provide structured threat analysis and user-oriented feedback.

III. PROPOSED SYATEM

The proposed system is a web-based intelligent scam and phishing detection platform designed to analyze textual input and identify potential cyber fraud threats using a rule-driven risk scoring mechanism. The system is developed using HTML, CSS, and Bootstrap for frontend interface design, while Python is used for backend processing and logical analysis. The objective of the system is to provide real-time detection, classification, and preventive guidance for suspicious messages.

A. System Overview

The system allows users to enter a message or suspicious text into a web interface. Once the input is submitted, it is transmitted to the backend server where a structured rule-based evaluation process is performed. The system analyzes the content using predefined logical rules and assigns a cumulative risk score based on detected indicators.
The overall workflow of the system is as follows:

- User inputs suspicious message.
- Backend processes the message using logical inference rules.
- Risk score is calculated based on detected indicators.
- Message is classified as Safe, Suspicious, or Scam.
- System generates detection reason, scam category, and safety suggestions.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, February 2026
Impact Factor: 8.2

- Result is stored securely in the database with encryption.

B. Risk Scoring Mechanism

The core component of the proposed system is the rule-driven risk scoring engine. Instead of relying on machine learning algorithms, the system evaluates predefined suspicious indicators and assigns weighted scores to each detected pattern. Examples of risk indicators include:

- Sensitive keywords (e.g., "OTP", "password", "bank account")
- Urgency triggers (e.g., "urgent", "immediately", "limited time")
- Reward-based terms (e.g., "lottery", "winner", "prize")
- Suspicious shortened URLs (e.g., bit.ly, tinyurl)

Payment request phrases

Each detected indicator contributes a specific weight to the total risk score. Based on the cumulative score, the system performs classification:

Low score → Safe

Medium score → Suspicious

High score → Scam

This structured scoring approach improves detection reliability while maintaining transparency.

C. Scam Category Classification

The system includes a category identification module that classifies detected scams into predefined categories such as:

Banking Scam

Lottery Fraud

Job Scam

Investment Fraud

General Phishing

Category classification is performed based on keyword clusters and contextual matching.

D. Reason Generation and Safety Suggestion

To enhance user understanding, the system generates a detailed explanation of why the message was flagged. The reason generation module identifies the specific indicators that triggered detection. Additionally, the system provides safety recommendations based on the detected category, such as advising users not to share confidential information or avoid clicking suspicious links.

E. Data Storage and Security

The system maintains a history of analyzed messages along with their classification results and timestamps. To ensure data security, sensitive information is encrypted before storage. This feature enhances system reliability and protects user privacy.The proposed architecture integrates logical inference, risk scoring, classification, and secure storage into a unified web-based platform. The design emphasizes simplicity, interpretability, and practical applicability in real-world cyber fraud detection scenarios.

IV. SYSTEM ARCHITECTURE

The system architecture of the proposed web-based scam and phishing detection system follows a structured client–server model. The architecture is designed to ensure efficient data processing, logical evaluation, and secure storage.

A. Architectural Overview

The system consists of three primary layers:

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, February 2026
Impact Factor: 8.2

- Presentation Layer (Frontend)
- Application Layer (Backend Logic Engine)
- Data Storage Layer (Database with Encryption)

The Presentation Layer is developed using HTML, CSS, and Bootstrap. It provides a user-friendly interface where users can enter suspicious messages and view detection results.The Application Layer is implemented using Python. It processes user input, executes logical inference rules, calculates risk scores, determines scam categories, generates explanations, and prepares safety suggestions.The Data Storage Layer maintains historical records of analyzed messages. Before storing data, encryption mechanisms are applied to ensure confidentiality and integrity.

B. Working Flow of the System

The operational workflow of the system can be summarized as follows:

- User submits text through the web interface.
- Backend receives and preprocesses the input.
- Risk scoring engine evaluates suspicious indicators.
- Classification module determines risk level.
- Reason generation module identifies triggering factors.
- Safety suggestion module provides preventive advice.
- Encrypted results are stored in the database.
- Final output is displayed to the user.

C. Architectural Advantages

The proposed architecture offers several advantages:

- Lightweight implementation without heavy computational requirements.
- Transparent decision-making through logical inference.
- Easy integration into web-based environments.
- Enhanced data security through encryption mechanisms.

The architecture ensures that the system remains scalable, interpretable, and suitable for real-time scam detection applications.

V. IMPLEMENTATION AND TESTING

The proposed web-based scam and phishing detection system was implemented using a structured development approach integrating frontend design, backend processing, logical inference mechanisms, and secure data storage.

A. Implementation Details

The frontend interface was developed using HTML, CSS, and Bootstrap to provide a responsive and user-friendly environment. The interface allows users to input suspicious messages and instantly view classification results, reasons for detection, scam category, and safety recommendations.The backend logic was implemented using Python. The core component of the system is the rule-driven risk scoring engine, which evaluates textual input against predefined suspicious indicators. The backend performs the following operations:

Text preprocessing (conversion to lowercase, removal of unnecessary characters)

- Keyword pattern matching
- Suspicious URL detection
- Risk score calculation based on weighted indicators
- Classification into Safe, Suspicious, or Scam categories
- Generation of detection reasoning

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, February 2026
Impact Factor: 8.2

- Scam category identification
- Safety recommendation generation

The system uses structured conditional statements and logical operators to ensure consistent and interpretable decision-making.For data management, a lightweight database is integrated to store analyzed messages along with their risk scores, categories, timestamps, and results. To enhance security, sensitive data is encrypted before storage using standard encryption techniques implemented in Python.

B. Testing Procedure

To evaluate system performance, multiple test cases were designed consisting of both legitimate and fraudulent message samples. The testing dataset included:

- Banking-related scam messages
- Lottery and prize fraud messages
- Job offer scams
- Investment fraud messages
- Genuine non-malicious messages

Each test input was processed through the system to verify classification accuracy, proper risk score calculation, and correct category identification.

C. Testing Results

The system successfully identified suspicious indicators such as urgency-based phrases, sensitive financial keywords, and shortened URLs. Messages containing multiple high-risk indicators were consistently classified as Scam, while messages with moderate indicators were marked as Suspicious. Genuine messages with no suspicious patterns were classified as Safe.

The testing phase confirmed that:

- The risk scoring mechanism functioned correctly.
- Classification thresholds were properly implemented.
- Reason generation provided accurate explanations.
- Scam category detection aligned with detected keywords.
- Encryption and history storage operated securely.

The implemented system demonstrated reliable detection performance under controlled testing scenarios and maintained stable operation during multiple input evaluations.

VI. RESULT AND ANALYSIS

The implemented web-based scam and phishing detection system was evaluated using multiple test inputs representing both fraudulent and legitimate communication scenarios. The primary objective of testing was to analyze the effectiveness of the rule-driven risk scoring mechanism and logical classification process.During evaluation, the system successfully detected high-risk messages containing combinations of sensitive keywords, urgency triggers, reward-based phrases, and suspicious URLs. Messages that included multiple high-weight indicators consistently produced higher cumulative risk scores and were accurately classified under the “Scam” category. Inputs with limited suspicious elements were categorized as “Suspicious,” while messages lacking risk indicators were correctly identified as “Safe.”The risk scoring mechanism proved effective in differentiating between varying levels of threat intensity. By assigning weighted values to different indicators, the system was able to prioritize high-risk patterns such as financial credential requests and shortened URLs. This structured approach reduced false classification and improved consistency in detection outcomes. The reason generation module enhanced interpretability by clearly indicating the factors responsible for classification decisions. This feature contributes significantly to user awareness, as individuals can understand why a particular message is considered suspicious. Additionally, the scam categorization module correctly grouped fraudulent messages into

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, February 2026 Impact Factor: 8.2

predefined categories such as Banking Scam, Lottery Fraud, Job Scam, and Investment Fraud.From a performance perspective, the system demonstrated stable response times during multiple input evaluations. The lightweight rule-based architecture ensured minimal computational overhead, making the system suitable for real-time web-based deployment. Furthermore, the integration of encrypted storage enhanced data security without affecting processing efficiency.Overall, the results indicate that the proposed rule-driven intelligent detection system provides a practical, interpretable, and efficient solution for identifying scam and phishing attempts in textual communication. While the system does not rely on complex machine learning models, it achieves reliable detection performance through structured logical inference and risk-based analysis.

VII. CONCLUSION

The rapid increase in online communication and digital transactions has significantly elevated the risk of scam and phishing attacks. Traditional manual detection methods are often insufficient to identify evolving fraud patterns. This paper presented the design and implementation of a web-based intelligent scam and phishing detection system using a rule-driven risk scoring mechanism and logical inference techniques.The proposed system analyzes textual input by evaluating predefined suspicious indicators such as sensitive keywords, urgency triggers, reward-based phrases, and suspicious URLs. Based on weighted scoring, the system classifies messages into Safe, Suspicious, or Scam categories. In addition to detection, the system provides reason generation, scam category identification, safety recommendations, encrypted data storage, and historical record management. These integrated features enhance transparency, user awareness, and overall cybersecurity protection.The implemented solution demonstrates that a structured rule-based approach can provide effective and interpretable detection performance without relying on computationally intensive machine learning models. The lightweight architecture ensures real-time response and ease of deployment in web-based environments.Future enhancements may include integration of machine learning algorithms for adaptive threat detection, expansion of keyword databases, incorporation of URL reputation analysis, and deployment as a browser extension or mobile application. Such improvements can further strengthen the system's detection capability and scalability.

In conclusion, the developed web-based intelligent scam and phishing detection system provides a practical, secure, and user-oriented approach for early identification of cyber fraud threats.

ACKNOWLEDGMENT

We would like to express our sincere gratitude to our project guide, Prof. Rahul Lilhare, for his continuous guidance, valuable suggestions, and constant support throughout the development of this project. His technical insights and encouragement helped us in understanding the practical aspects of system design and implementation. We are also thankful to the Department of Computer Application, KDK College of Engineering, Nagpur, for providing the necessary resources and academic environment to successfully carry out this work. Finally, we extend our appreciation to our classmates and well-wishers who directly or indirectly contributed to the completion of this project.

REFERENCES

[1]. A. K. Jain and B. B. Gupta, "Phishing detection: Analysis of visual similarity based approaches," Security and Communication Networks, vol. 2017, pp. 1–20, 2017.
[2]. R. Verma and A. Das, "What's in a URL: Fast feature extraction and malicious URL detection," in Proc. IEEE International Conference on Cyber Security, 2017, pp. 55–63.
[3]. S. Marchal, J. Francois, R. State, and T. Engel, "PhishStorm: Detecting phishing with streaming analytics," IEEE Transactions on Network and Service Management, vol. 11, no. 4, pp. 458–471, Dec. 2014.
[4]. M. A. Rajab, L. Ballard, N. Mavrommatis, and P. Snyder, "The Nocebo Effect on the Web: An Analysis of Fake Antivirus Distribution," in Proc. USENIX Workshop on Large-Scale Exploits and Emergent Threats, 2010, pp. 1–8.
[5]. T. Moore and R. Clayton, "Examining the impact of website take-down on phishing," in Proc. Anti-Phishing Working Groups eCrime Researchers Summit, 2007, pp. 1–13.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, February 2026
Impact Factor: 8.2

[6]. C. Whittaker, B. Ryner, and M. Nazif, "Large-scale automatic classification of phishing pages," in Proc. Network and Distributed System Security Symposium (NDSS), 2010.
[7]. D. Gupta, S. Singhal, and A. Kapoor, "A literature survey on social engineering attacks: Phishing attack," in Proc. International Conference on Computing, Communication and Automation, 2016, pp. 537–540.
[8]. W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed. Pearson Education, 2017.
[9]. N. Chou, R. Ledesma, Y. Teraguchi, and D. Boneh, "Client-side defense against web-based identity theft," in Proc. Network and Distributed System Security Symposium (NDSS), 2004.
[10]. S. Sheng, B. Wardman, G. Warner, L. Cranor, J. Hong, and C. Zhang, "An empirical analysis of phishing blacklists," in Proc. Conference on Email and Anti-Spam (CEAS), 2009.