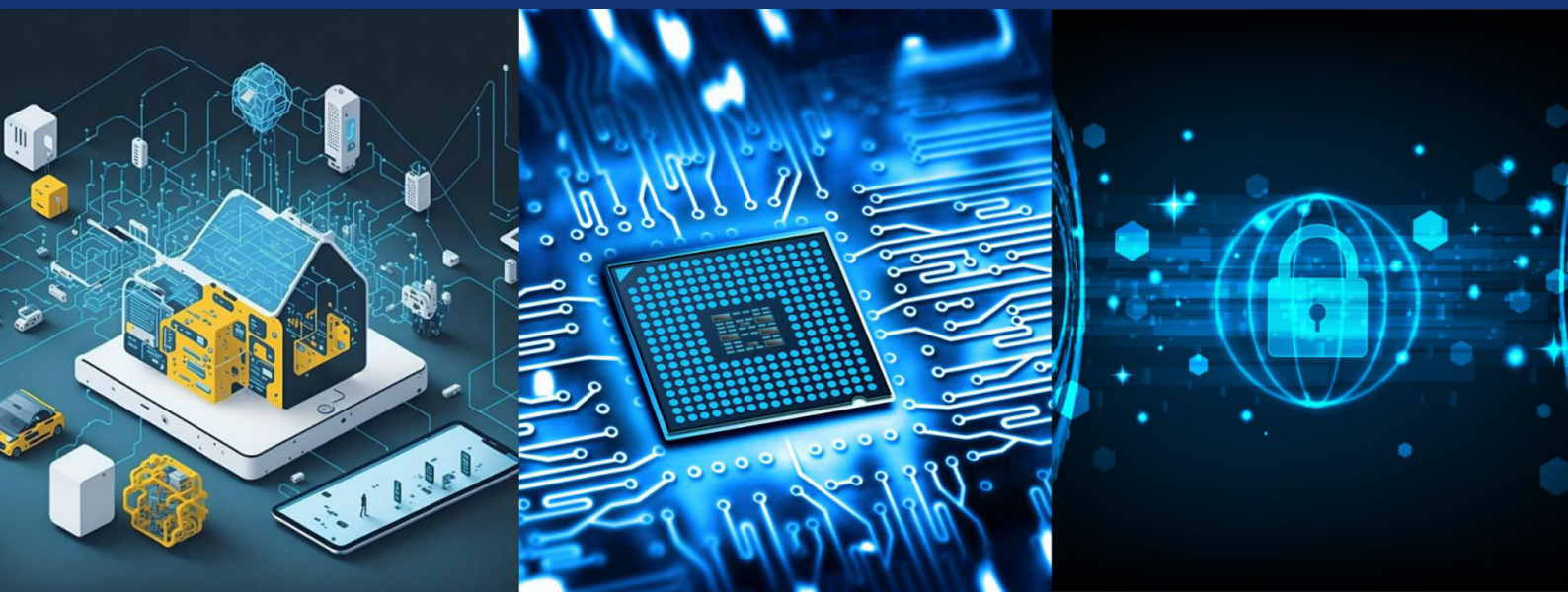
IJIRCCE

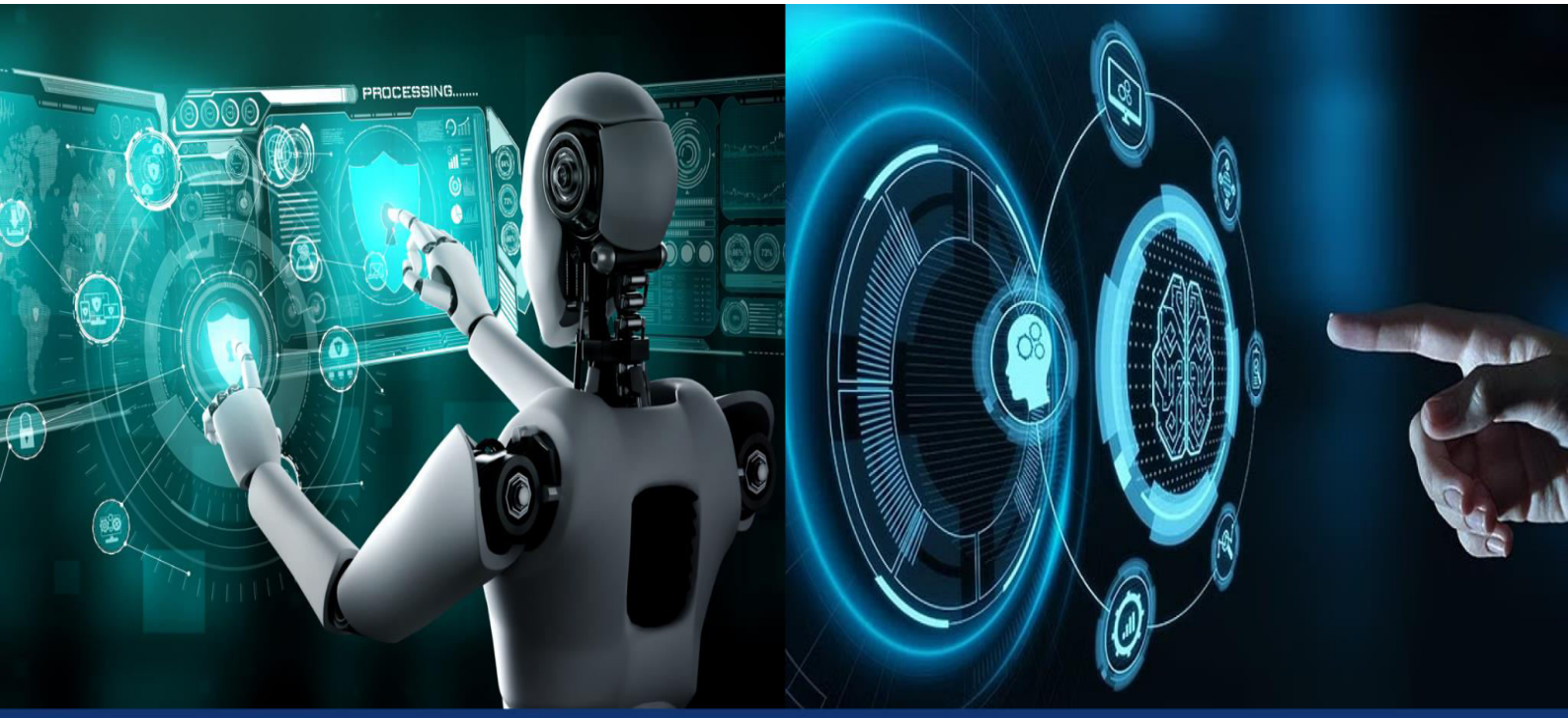
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.927

Volume 14, Issue 7, July 2026

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407034

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Unified Threat Detection and Mitigation Framework for QRishing and Card Skimming Attacks

Putta Vamshi, Dr.V.Uma Rani

Post-Graduate Student, Department of Computer Science Engineering, Computer Networks and Information Security, Jawaharlal Nehru Technological University, Hyderabad, India

Professor, Department of Computer Science Engineering, Jawaharlal Nehru Technological University, Hyderabad, India

ABSTRACT: The rapid growth of digital payment systems has increased the use of QR code payments and point-of-sale (POS) transactions in retail and public environments. however, these technologies are vulnerable to cyber threats such as QRishing and card skimming attacks, which can result in financial losses and compromise sensitive user information. this paper presents a **Unified Threat Detection and Mitigation Framework (UTDMF)** for detecting fraudulent QR codes and suspicious POS transactions using machine learning techniques. the framework consists of data collection, preprocessing, QR threat analysis, POS fraud detection, risk scoring, and alert generation modules. QR code features and transaction attributes are analyzed to classify activities as legitimate or fraudulent. the system provides real-time threat detection, unified risk assessment, and security alerts through an interactive dashboard. experimental results demonstrate the effectiveness of the proposed framework in identifying QR-based phishing attacks and POS fraud with high accuracy. the proposed solution enhances digital payment security and supports proactive fraud prevention in modern payment environments.

KEYWORDS: Card Skimming, POS Fraud Detection, Machine Learning, Digital Payment Security, Risk Scoring, Cybersecurity.

I. INTRODUCTION

Digital payment systems have become an essential part of modern transactions. QR code payments and Point-of-Sale (POS) card transactions are widely used in retail stores, public services, and online platforms due to their convenience and speed. However, the increasing use of these technologies has also led to the rise of cyber threats such as QRishing and card skimming attacks. This project proposes a Unified Threat Detection and Mitigation Framework (UTDMF) that utilizes machine learning techniques to detect fraudulent QR codes and suspicious POS transactions. The system helps improve payment security by identifying threats and generating timely alerts.

Traditional fraud detection approaches often focus on individual attack types and may not effectively identify multiple threats occurring across different payment channels. As digital payment ecosystems continue to expand, there is a growing need for an integrated security framework capable of detecting and mitigating diverse fraud activities in real time. Machine learning techniques have demonstrated significant potential in identifying suspicious patterns, analyzing transaction behavior, and improving fraud detection accuracy.

II. RELATED WORK

A. QRishing Detection and QR Code Security

Jurgensen and Hoepman (2022) investigated the growing threat of QRishing attacks and analyzed how smartphone users interact with QR codes in real-world environments. Their study showed that users often trust QR codes without verifying embedded URLs, making them vulnerable to phishing attacks. The research highlighted the importance of user awareness and intelligent QR code verification mechanisms for improving security against QR-based cyber threats.

B. Machine Learning-Based Phishing Detection

Sahingoz et al. (2019) proposed a machine learning-based phishing detection framework using URL features and classification techniques. The system analyzed characteristics such as URL length, domain information, and suspicious

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

patterns to identify malicious websites. Experimental results demonstrated that machine learning models can effectively distinguish phishing URLs from legitimate websites with high accuracy, making them suitable for QR threat detection systems.

C. Fraud Detection in Financial Transactions

Almashhadani et al. (2023) presented a comprehensive survey on machine learning-based fraud detection systems in financial transactions. The study reviewed various classification algorithms and demonstrated that intelligent fraud detection models can identify suspicious transaction patterns, reduce financial losses, and improve payment security. Their work emphasized the growing importance of automated fraud detection in digital payment ecosystems.

D. Machine Learning for Cybersecurity and Fraud Analysis

Sarker (2023) reviewed machine learning techniques for fraud detection and cybersecurity applications. The research highlighted the ability of machine learning algorithms to learn behavioral patterns from large datasets and accurately classify fraudulent activities. The study showed that intelligent security systems can significantly improve threat detection performance while reducing false alarms in financial and cybersecurity environments.

E. Credit Card Fraud Detection Using Data Mining

Bhattacharyya et al. (2011) conducted a comparative study on credit card fraud detection using data mining techniques. Their work demonstrated that transaction analysis based on attributes such as transaction amount, location, and user behavior can effectively identify fraudulent activities. The study confirmed that data-driven fraud detection approaches provide better accuracy and reliability compared to traditional rule-based methods.

III. PROPOSED ALGORITHM

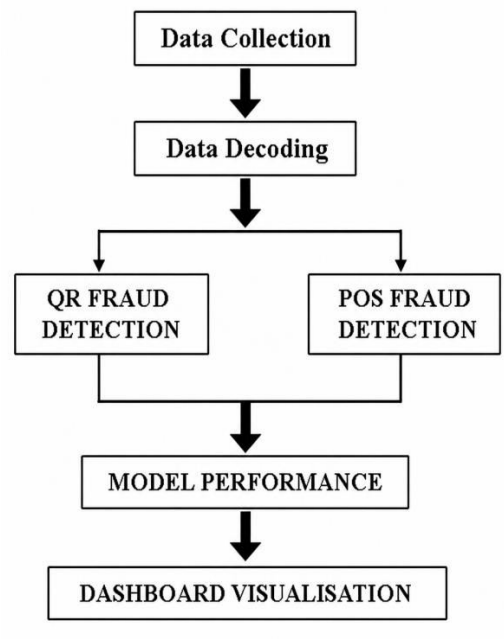


Figure 1: proposed Architecture

A. Design Considerations

- The proposed system uses **QR Code Dataset** and **POS Transaction Dataset** collected from retail and public payment environments.
- QR transaction data is decoded to extract important attributes such as URL information, QR content, domain characteristics, and transaction details.
- POS transaction records are analyzed using attributes such as transaction amount, transaction time, location, card age, and failed PIN attempts.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- Data preprocessing techniques including cleaning, validation, and normalization are applied to improve data quality and model performance.
- The datasets are divided into **training and testing sets using a 70:30 ratio**.
- Machine Learning classification models are used separately for **QR Fraud Detection** and **POS Fraud Detection**.
- A unified risk scoring mechanism combines QR fraud probability and POS fraud probability to generate a final fraud risk score.
- System performance is evaluated using **Accuracy, Precision, Recall, F1-Score, and Confusion Matrix**.

B. Description of the Proposed Algorithm

The objective of the proposed algorithm is to identify fraudulent activities related to QRishing attacks and Card Skimming attacks by analyzing QR code transactions and POS transaction data. The proposed methodology consists of three major steps.

Step 1: Data Preprocessing

The QR Code Dataset and POS Transaction Dataset are collected and preprocessed. Invalid records, missing values, and redundant attributes are removed. Data normalization is performed to improve prediction accuracy.

The fraud classification labels are represented as:

Classification = {1, Fraud ; 0, Legitimate} ..... (1)

Data normalization is performed using:

where:

- **X** = Original feature value
- **μ** = Mean of feature values
- **σ** = Standard deviation of feature values

Step 2: QR and POS Fraud Detection Model

The preprocessed datasets are divided into training and testing datasets. Separate machine learning models are trained for QR fraud detection and POS fraud detection.

QR Fraud Detection

The QR detection model analyzes:

- QR Content
- URL Features
- Domain Characteristics
- Encoded Information

The prediction function is represented as:

ŷQR = fQR(XQR) ..... (2)

where:

- **XQR** = QR feature vector
- **ŷQR** = Predicted QR fraud label
- **fQR(XQR)** = Trained QR fraud detection model

POS Fraud Detection

The POS detection model analyzes:

- Transaction Amount
- Transaction Time
- Transaction Location
- Card Age
- Failed PIN Attempts

The prediction function is represented as:

ŷPOS = fPOS(XPOS) ..... (3)

where:

- **XPOS** = POS feature vector
- **ŷPOS** = Predicted POS fraud label
- **fPOS(XPOS)** = Trained POS fraud detection model

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Step 3: Performance Evaluation

The trained models are evaluated using standard classification metrics.

Accuracy = (TP + TN) / (TP + TN + FP + FN) ..... (4)

Precision = TP / (TP + FP) ..... (5)

Recall = TP / (TP + FN) ..... (6)

F1-Score = 2 × (Precision × Recall) / (Precision + Recall) ..... (7)

where:

TP = True Positives

TN = True Negatives

FP = False Positives

FN = False Negatives

Based on the calculated fraud probability and risk score, the system generates alerts for suspicious transactions. High-risk transactions trigger immediate notifications through the dashboard, enabling analysts to take appropriate fraud mitigation actions. Experimental results demonstrate that the proposed **Unified Threat Detection and Fraud Mitigation Framework (UTDMF)** effectively detects QRishing and Card Skimming attacks while maintaining high classification accuracy and reliable fraud prevention.

IV. PSEUDO CODE

Step 1: Load the QR Code Dataset and POS Transaction Dataset.
Step 2: Preprocess the datasets.
  a) Remove invalid and redundant records.
  b) Perform data cleaning and validation.
Step 3: Split the datasets into Training Set (70%) and Testing Set (30%).
Step 4: Perform QR Data Decoding.
  a) Decode QR code content.
  b) Extract URL and domain information.
  c) Extract transaction-related attributes.
Step 5: Train the QR Fraud Detection Model.
  a) Extract QR fraud features.
  b) Train the machine learning classifier.
  c) Predict QR fraud probability.
  d) Classify QR transaction as Legitimate or Fraudulent.
Step 6: Train the POS Fraud Detection Model.
  a) Extract POS transaction features.
    - Transaction Amount
    - Transaction Time
    - Transaction Location
    - Card Age
    - Failed PIN Attempts
  b) Train the machine learning classifier.
  c) Predict POS fraud probability.
  d) Classify POS transaction as Legitimate or Fraudulent.
Step 7: Evaluate model performance.
  a) Calculate Accuracy.
  b) Calculate Precision.
  c) Calculate Recall.
  d) Calculate F1-Score.
  e) Generate Confusion Matrix.
Step 8: Generate fraud alerts.
  a) Identify suspicious transactions.
  b) Generate alerts for High-Risk activities.
  c) Send notifications to dashboard users.
Step 9: Display results through Dashboard Visualization.
  a) Fraud Classification Results.

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407034

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

b) Performance Metrics.

Step 10: End.

V. SIMULATION RESULTS

The simulation studies were conducted using QR code and POS transaction datasets collected from retail and public environments. The proposed Unified Threat Detection and Fraud Mitigation Framework was implemented using Python and Scikit-learn. During preprocessing, QR code information was decoded, transaction attributes were extracted, and feature scaling was applied to normalize the dataset. The processed dataset was then divided into training and testing sets using a 70:30 ratio for model development and evaluation.

The proposed framework was evaluated using Random Forest, XGBoost, and Support Vector Machine (SVM) classifiers. Performance was measured using accuracy, precision, recall, F1-score, and confusion matrix analysis. The experimental results show that all machine learning models achieved high classification performance in distinguishing fraudulent and legitimate activities. Among the evaluated models, the Random Forest classifier provided the most consistent and reliable results. The findings demonstrate that machine learning significantly improves fraud detection capability, reduces classification errors, and provides a robust solution for identifying both QRishing and card skimming attacks.

Figure 2: Confusion Matrix Analysis and Feature Importance Comparison of Machine Learning Models

The confusion matrices illustrate the classification performance of the Random Forest, XGBoost, and Support Vector Machine (SVM) models by showing the distribution of correctly and incorrectly classified fraudulent and legitimate transactions. The results indicate that all three machine learning models achieve high fraud detection accuracy with very low misclassification rates. The feature importance analysis generated by the Random Forest model identifies failed attempts, transaction distance, card age, and transaction amount as the most influential factors in fraud prediction. These findings demonstrate the effectiveness of the proposed Unified Threat Detection and Fraud Mitigation Framework in accurately detecting QRishing and card skimming attacks while minimizing false alarms.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

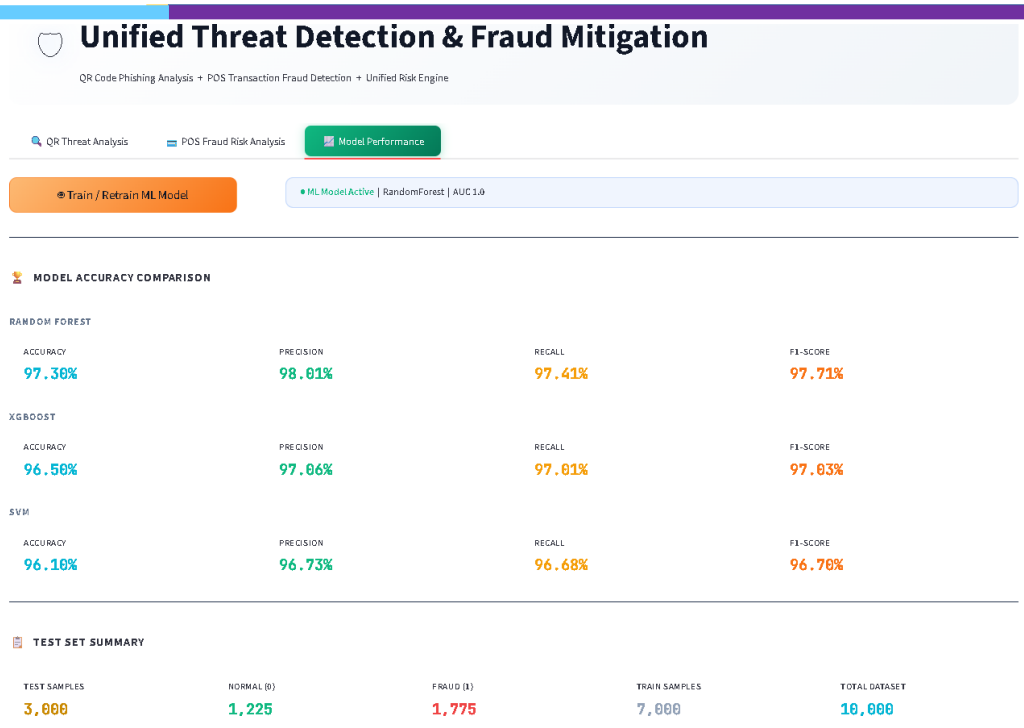
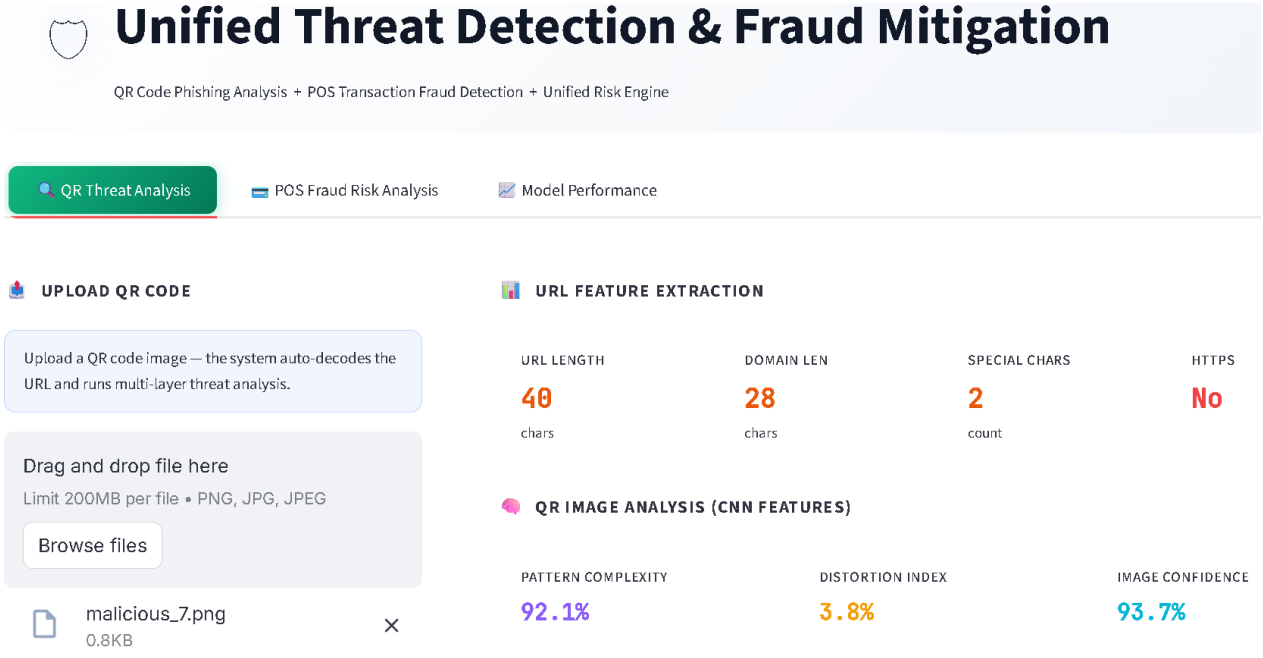


Figure 3: *Model Performance Comparison Results*

The model performance comparison presents the Accuracy, Precision, Recall, and F1-Score achieved by the Random Forest, XGBoost, and Support Vector Machine (SVM) classifiers. The results indicate that all models achieved high classification performance in distinguishing fraudulent and legitimate transactions. Among the evaluated models, the Random Forest classifier achieved the highest accuracy and overall performance, demonstrating its effectiveness for fraud detection. The findings confirm that machine learning-based classification provides reliable detection of QRishing and card skimming attacks while maintaining low classification errors.QRishing and card skimming attacks



© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407034

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

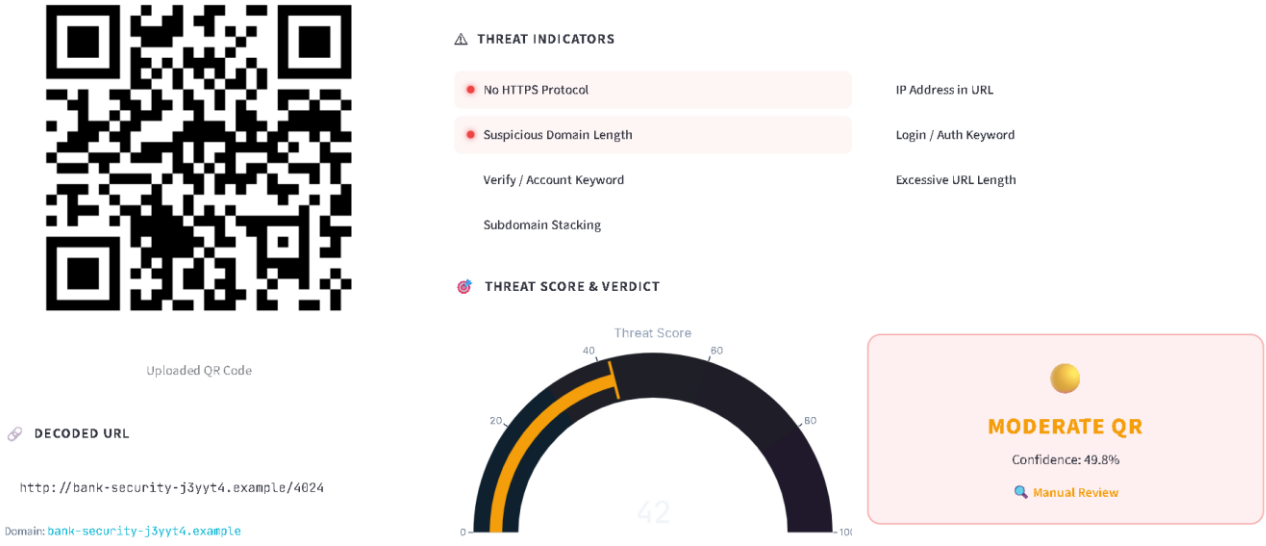


Figure 4: QR Code Threat Analysis and Detection Result

The figure illustrates the complete QR Threat Analysis process of the proposed Unified Threat Detection and Fraud Mitigation Framework. The uploaded QR code is decoded, URL and image-based features are extracted, and multiple threat indicators are evaluated to calculate a threat score. Based on the detected suspicious characteristics, including the absence of HTTPS and suspicious domain attributes, the framework classifies the QR code as Moderate Risk and recommends manual review before use.

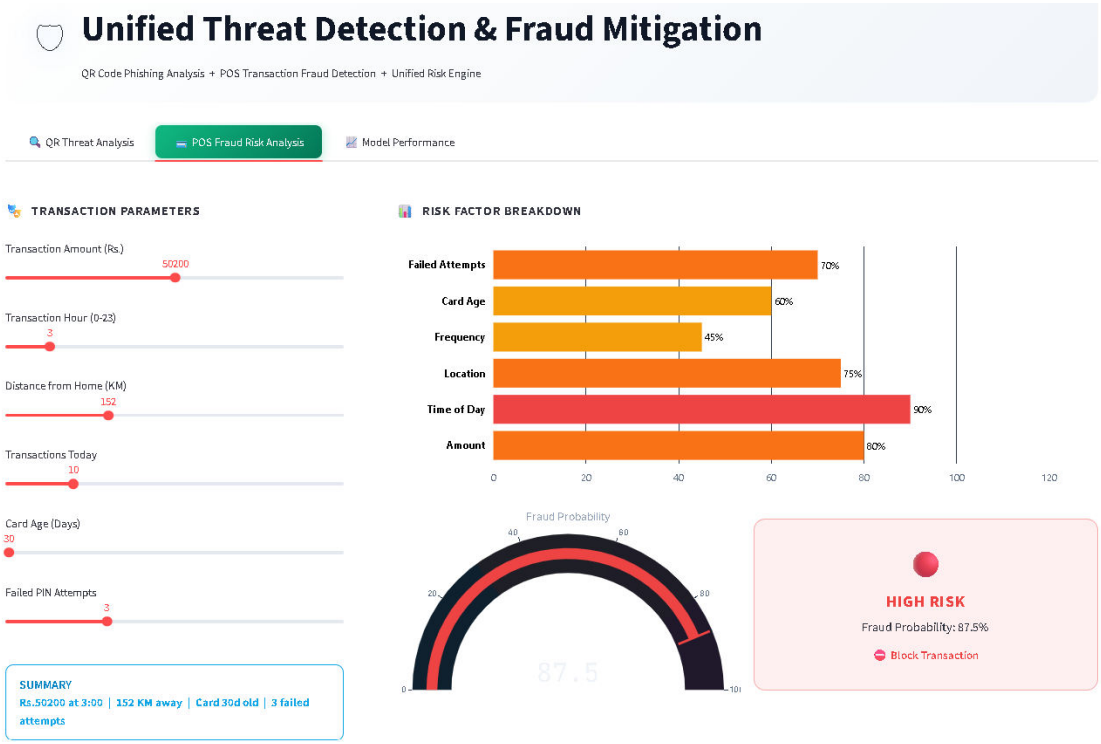


Fig. 5: High-Risk POS Transaction Detection Result

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Model	Accuracy	Precision	Recall	F1-Score
Random Forest	0.973	0.9801	0.9741	0.9771
XGBoost	0.965	0.9706	0.9701	0.9703
SVM	0.961	0.9673	0.9668	0.9670

Table 1: Performance Comparison of Machine Learning Models for QRishing and Card Skimming Detection

The table presents the performance metrics of the machine learning models used for QR phishing detection and POS transaction fraud analysis. The results show that Random Forest achieved the highest performance with 97.30% accuracy, 98.01% precision, 97.41% recall, and 97.71% F1-score, while XGBoost and SVM also demonstrated excellent threat detection capability with very high evaluation scores, confirming the effectiveness of the proposed Unified Threat Detection and Fraud Mitigation framework.

VI. CONCLUSION AND FUTURE WORK

The proposed Unified Threat Detection and Fraud Mitigation Framework (UTDMF) provides an effective solution for detecting QRishing attacks and card skimming fraud using machine learning techniques. The system combines QR code analysis, POS transaction monitoring, feature extraction, and classification models to accurately identify suspicious activities. Experimental results demonstrate that the framework achieves high accuracy, precision, recall, and F1-score, with Random Forest providing the best performance. The modular architecture improves scalability, maintainability, and reliability, making the system suitable for real-world cybersecurity applications. Overall, the framework enhances digital payment security by reducing fraud risks and improving threat detection capabilities.

In the future, the framework can be enhanced by integrating advanced deep learning models and real-time threat intelligence mechanisms. Support for additional fraud types such as mobile payment fraud, phishing websites, and identity theft can further expand its capabilities. Integration with cloud platforms and adaptive learning techniques will improve scalability and enable continuous detection of emerging cyber threats, making the system more robust and effective in securing digital transactions.

REFERENCES

[1] M. Jurgensen and J. H. Hoepman, 'QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks', Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroSPW), pp. 128–137, 2022.
[2] O. K. Sahingoz, E. Buber, O. Demir and B. Diri, 'Machine Learning Based Phishing Detection from URLs', Expert Systems with Applications, Vol. 117, pp. 345–357, 2019.
[3] A. O. Almashhadani, M. Kaiiali, S. Sezer and P. O'Kane, 'Machine Learning Based Fraud Detection Systems in Financial Transactions: A Survey', IEEE Access, Vol. 11, pp. 56782–56805, 2023.
[4] I. H. Sarker, 'Machine Learning for Intelligent Fraud Detection in Financial and Cyber Security Systems: A Comprehensive Review', Journal of Network and Computer Applications, Vol. 215, pp. 103623, 2023.
[5] S. Bhattacharyya, S. Jha, K. Tharakunnel and J. C. Westland, 'Data Mining for Credit Card Fraud: A Comparative Study', Decision Support Systems, Vol. 50, Issue 3, pp. 602–613, 2011.
[6] L. Alzubaidi, J. Zhang, A. J. Humaidi et al., 'Review of Machine Learning and Deep Learning Techniques for Cybersecurity and Fraud Detection', IEEE Access, Vol. 11, pp. 74521–74545, 2023.
[7] A. Dal Pozzolo, O. Caelen, R. A. Johnson and G. Bontempi, 'Calibrating Probability with Undersampling for Unbalanced Classification', IEEE Symposium Series on Computational Intelligence (SSCI), pp. 159–166, 2015.
[8] A. C. Bahnsen, D. Aouada and B. Ottersten, 'Example-Dependent Cost-Sensitive Decision Trees for Credit Card Fraud Detection', Expert Systems with Applications, Vol. 42, Issue 19, pp. 6609–6619, 2015.
[9] A. K. Jain and B. B. Gupta, 'Phishing Detection: Analysis of Visual Similarity Based Approaches', Security and Communication Networks, Vol. 10, Issue 13, pp. 2168–2185, 2017.
[10] R. M. Mohammad, F. Thabtah and L. McCluskey, 'Predicting Phishing Websites Based on Self-Structuring Neural Network', Neural Computing and Applications, Vol. 25, Issue 2, pp. 443–458, 2014.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details