International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 03(March),2026
Received: 06-02-2026 Accepted: 07-03-2026 Published: 20-03-2026

SCAM-VISION: HYBRID AI-BASED REAL-TIME DETECTION OF FRAUDULENT UPI IDS, SUSPICIOUS PHONE NUMBERS, AND QR CODE PAYMENT SCAMS

Rajakumar Varshitha[1], Pedamutti Rajesh[2],Veeranki Vasavi[3], Shaik Nazeer[4], Reddy Nandini[5]

[1] Dept. of CSE, SR Gudlavalleru Engineering College, Gudlavalleru, Andhra Pradesh, India, **varshitha3114@gmail.com**.
[2] Assistant Professor, Dept. of CSE, SR Gudlavalleru Engineering College, Gudlavalleru, Andhra Pradesh, India.
[3] Dept. of CSE, SR Gudlavalleru Engineering College, Gudlavalleru, Andhra Pradesh, India.
[4] Dept. of CSE, SR Gudlavalleru Engineering College, Gudlavalleru, Andhra Pradesh, India.
[5] Dept. of CSE, SR Gudlavalleru Engineering College, Gudlavalleru, Andhra Pradesh, India.

Abstract— The rapid growth of digital payment systems has significantly increased the risk of financial fraud, particularly through fraudulent Unified Payments Interface (UPI) IDs and deceptive phone numbers. Traditional fraud detection methods often rely on static rule-based systems, which fail to identify newly evolving scam patterns. This paper presents SCAM-VISION, a real-time, AI-driven hybrid fraud detection framework designed to identify suspicious UPI identifiers and phone numbers with high accuracy. The proposed system integrates three complementary detection layers: rule-based keyword analysis, trusted database verification, and deep learning-based anomaly detection using a Variational Autoencoder (VAE). Character-level TF-IDF vectorization is employed to capture structural patterns in legitimate UPI handles, enabling the VAE to detect subtle deviations commonly used in scam identifiers. Additionally, phone number verification is enhanced through carrier and line-type analysis to detect VoIP-based and foreign scam numbers. SCAM-VISION supports QR code scanning for automatic UPI extraction and provides a real-time web dashboard that displays risk scores, detection reasons, and performance metrics. Experimental evaluation demonstrates that the hybrid approach significantly improves detection reliability compared to standalone rule-based methods, achieving higher precision and reduced false positives. The system is lightweight, scalable, and suitable for real-world deployment, offering an effective solution for enhancing digital payment security.

Keywords— Scam Detection, UPI Fraud, Anomaly Detection, Variational Autoencoder, Financial Cybersecurity, Machine Learning, QR Code Analysis, Real-Time Fraud Prevention

I. INTRODUCTION

Digital payment platforms have transformed the way financial transactions are performed by offering speed, convenience, and accessibility. The rapid growth of online and mobile-based financial services has significantly increased transaction volumes, making digital payments a critical component of modern economies. However, this expansion has also introduced new security challenges, particularly in the form of financial fraud and cyber-enabled scams [1][2]. In India, the Unified Payments Interface (UPI) has emerged as one of the most widely adopted real-time payment systems due to its simplicity and interoperability, but its widespread use has also made it an attractive target for fraudsters [9]. Fraudsters increasingly exploit fake UPI IDs, misleading QR codes, and suspicious phone numbers to deceive users into transferring money or revealing sensitive information. Existing fraud detection mechanisms in digital payment systems largely rely on predefined rules, blacklists, and manual verification processes [4][7]. While such approaches are effective in identifying previously known scam patterns, they struggle to detect newly evolving fraud techniques that are deliberately designed to bypass static rules and signature-based defenses [1][5]. As scammers continuously modify UPI identifiers by inserting deceptive keywords or altering character structures, traditional detection systems exhibit limited adaptability and higher false-negative rates. Recent advancements in artificial intelligence and machine learning have shown strong potential in addressing these cybersecurity challenges through intelligent feature extraction, preprocessing, and optimization techniques [8][11][12]. In particular, anomaly detection techniques have proven effective in identifying abnormal patterns without requiring large volumes of labeled fraudulent data [4][8]. Unsupervised and semi-supervised learning models are especially suitable for fraud detection scenarios, where genuine transactions vastly outnumber fraudulent ones and labeled scam data is scarce [7]. Deep learning models unseen fraud patterns [3][8]. Several studies have demonstrated the effectiveness of deep learning, adversarial learning, and optimized intelligent systems in anomaly detection and classification tasks across financial security, network monitoring, and pattern recognition domains [6][10][13][14][15]. Recent research also highlights the role of hybrid learning models, optimization-based feature selection,

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 03(March),2026
Received: 06-02-2026 Accepted: 07-03-2026 Published: 20-03-2026

and multimodal data analysis in improving robustness and detection accuracy in complex real-world environments [16][17][18]. When combined with traditional rule-based filtering and trusted entity verification, deep learning–based anomaly detection can significantly improve detection accuracy while reducing false positives [6][8]. Additionally, recent studies emphasize the importance of integrating multiple detection strategies, such as text-based identifier analysis, keyword detection, and telecom metadata verification, to effectively combat modern scam techniques [9][10][12].

II. Literature Review

The increasing use of digital payment systems has attracted significant research attention toward fraud and scam detection. Early studies in financial fraud detection primarily focused on rule-based and signature-based approaches, where predefined patterns, keywords, or blacklists were used to identify malicious activities. These methods are computationally efficient and easy to implement; however, their effectiveness is limited to known fraud patterns. As scammers continuously modify their strategies, rule-based systems often fail to detect novel or evolving attacks. To overcome these limitations, researchers introduced machine learning–based classification techniques such as Decision Trees, Support Vector Machines (SVM), Random Forests, and Logistic Regression. These models improved detection accuracy by learning patterns from historical transaction data. However, most supervised learning methods require large, well-labeled datasets, which are difficult to obtain in real-world fraud scenarios. Additionally, these models tend to degrade in performance when faced with imbalanced datasets, where genuine transactions significantly outnumber fraudulent ones. Recent research has shifted toward unsupervised and semi-supervised learning techniques, which are more suitable for fraud detection tasks where labeled scam data is scarce. Anomaly detection models learn the normal behavior of legitimate users and flag deviations as suspicious. Techniques such as Isolation Forests, One-Class SVMs, and Autoencoders have demonstrated promising results in identifying abnormal financial patterns without prior knowledge of fraud samples. Deep learning–based approaches, particularly Autoencoders and Variational Autoencoders (VAEs), have gained popularity due to their ability to capture complex, non-linear relationships in data. Several studies have shown that VAEs are effective in detecting subtle anomalies in structured and unstructured data, including transaction identifiers, payment handles, and communication metadata. By measuring reconstruction error, these models can identify inputs that significantly differ from learned legitimate patterns, making them suitable for detecting cleverly disguised scam identifiers.

In the context of UPI and mobile-based fraud, existing literature highlights the importance of combining multiple detection strategies. Research indicates that relying solely on transaction amounts or user behavior is insufficient, as many scams exploit social engineering rather than abnormal transaction values. Some studies propose combining text analysis of payment identifiers, keyword detection, and trusted entity verification to improve detection reliability. QR code–based fraud detection has also been explored, emphasizing the need for automated extraction and validation of embedded payment information. Despite these advancements, many existing systems lack real-time deployment capability or focus on a single detection technique. There remains a gap in developing hybrid frameworks that integrate rule-based logic, trusted database validation, and deep learning–based anomaly detection into a unified, scalable system. The proposed SCAM-VISION framework addresses this gap by combining lightweight heuristic checks with VAE-based anomaly detection and external phone verification, offering a more robust and adaptive solution for real-world digital payment fraud detection.

III. Existing System

Current fraud detection systems used in digital payment platforms mainly rely on rule-based mechanisms and blacklist-driven verification. These systems detect scams by checking predefined keywords such as “refund,” “KYC,” or “reward,” and by validating payment identifiers against stored lists of known fraudulent UPI IDs or phone numbers. While such approaches are fast and easy to implement, they are effective only for previously identified scam patterns and fail to adapt to new or modified fraud techniques. Many existing systems also employ manual verification or customer-reported feedback to update scam databases. This process introduces delays, during which fraudulent identifiers remain active and continue to exploit users. Furthermore, scammers frequently create new UPI handles by slightly altering characters or bank suffixes, allowing them to bypass static blacklists and continue fraudulent activities undetected. Some advanced platforms incorporate supervised machine learning models trained on historical transaction data to classify transactions as legitimate or fraudulent. Although these models improve accuracy compared to basic rule-based systems, they require large volumes of labeled data, which is often unavailable or highly imbalanced in real-world financial environments. As a result, these systems struggle with generalization and show reduced performance when encountering previously unseen scam patterns.Existing fraud detection solutions also tend to analyze transaction behavior or monetary patterns, such as transaction frequency or amount deviations. However, many UPI scams rely on social engineering rather than abnormal transaction values, making behavior-based detection insufficient. Additionally, most systems lack support for QR code-based UPI analysis, despite QR codes being a common medium for initiating fraudulent payments. Overall, the existing systems operate in a fragmented manner, using isolated detection techniques without coordination between rule-based logic, intelligent learning models, and trusted verification sources. This results in higher false positive rates, limited adaptability, and delayed scam identification. These limitations highlight the

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 03(March),2026
Received: 06-02-2026 Accepted: 07-03-2026 Published: 20-03-2026

need for a more integrated, adaptive, and real-time fraud detection system, capable of identifying both known and emerging scam patterns effectively.

IV. PROPOSED SYSTEM

From Figure 1, SCAM-VISION is illustrated as a hybrid AI-based framework designed to detect fraudulent UPI IDs and scam-related phone numbers in real time. The architecture shown in Figure 1 highlights how the system integrates multiple verification layers to improve detection accuracy, adaptability, and reliability, unlike traditional approaches that rely on a single detection method. As depicted in Figure 1, the system is specifically designed to identify both known

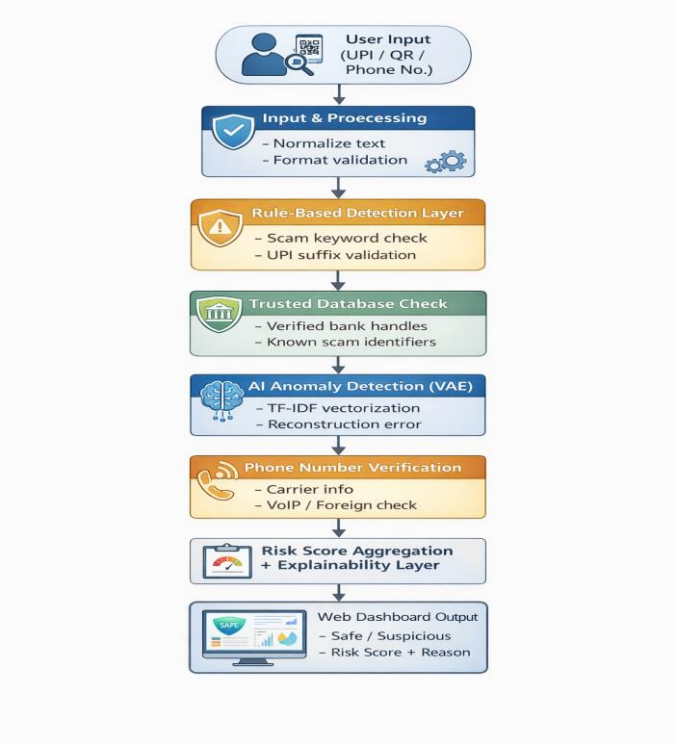

Fig. 1 SCAM-VISION: Hybrid AI-Based System Architecture for Real-Time Scam Detection

scam patterns and newly emerging fraudulent identifiers that bypass conventional rule-based checks. As shown in Figure 1, the first layer of the proposed system performs format validation and rule-based analysis. In this stage, the input UPI ID or phone number is checked for structural correctness and scanned for commonly used scam keywords such as “refund,” “verify,” and “reward.” In addition, the UPI handle suffix is validated against a trusted database of verified bank and service provider identifiers. This layer, illustrated in Figure 1, enables fast detection of obvious scam attempts with minimal computational overhead. The second layer, as presented in Figure 1, applies deep learning–based anomaly detection using a Variational Autoencoder (VAE). Character-level TF-IDF vectorization is used to convert UPI identifiers into numerical feature representations that capture structural and linguistic patterns. The VAE model is trained exclusively on legitimate UPI IDs, allowing it to learn normal behavior without requiring labeled fraud data. During inference, inputs that produce high reconstruction error are flagged as anomalous, indicating potential scam attempts that do not match learned legitimate patterns. For phone number analysis, Figure 1 shows the integration of carrier-level verification and line-type classification. This module identifies untrusted, VoIP-based, or foreign numbers that are commonly associated with scam operations. By combining telecom metadata with AI-based detection, the system provides a more reliable assessment of phone-based scam risks.

Furthermore, as depicted in Figure 1, SCAM-VISION supports QR code scanning, enabling automatic extraction and analysis of embedded UPI IDs from uploaded images or live camera input. This feature enhances user convenience and addresses a common attack vector used in real-world digital payment fraud. Finally, the architecture in Figure 1 demonstrates how the system generates a composite risk score based on outputs from all detection layers and presents clear explanations for each decision through a web-based dashboard that displays real-time results, detection reasons, and model performance metrics. The proposed framework is lightweight, scalable, and suitable for deployment in real-world digital payment environments, offering an effective and practical solution for enhancing financial transaction security.

V. COMPONENTS AND SOFTWARE DETAILS

The SCAM-VISION system is developed using a modular architecture that integrates multiple software components to ensure efficient real-time scam detection. Each component is designed to perform a specific function while maintaining seamless interaction with other modules. This modular design improves system scalability, maintainability, and performance.

A. Input and Preprocessing Module

This component accepts user inputs in the form of UPI IDs, phone numbers, or QR code images. The input data is first normalized by converting text to lowercase and removing unnecessary characters to maintain consistency. Format validation is applied to ensure that the UPI ID or phone number follows standard structural rules before further analysis. This step reduces false detections caused by invalid or malformed inputs.

B. Rule-Based Detection Module

The rule-based module performs fast initial screening by scanning inputs for commonly used scam keywords and suspicious patterns in Figure 3. It also verifies UPI handle suffixes against a trusted list of legitimate banks and service providers. This module is computationally lightweight and enables immediate detection of well-known scam patterns, making it suitable for real-time applications.

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 03(March),2026
Received: 06-02-2026 Accepted: 07-03-2026 Published: 20-03-2026

C. Anomaly Detection Module (VAE)

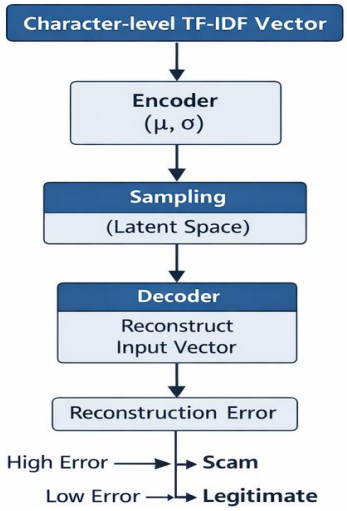

Fig. 2 VAE-Based Anomaly Detection Using Character-Level TF-IDF Features

The anomaly detection module is the core intelligence of the system, as illustrated in Figure 2. It uses a Variational Autoencoder (VAE) trained on legitimate UPI identifiers to learn normal structural patterns. As shown in Figure 2, character-level TF-IDF vectorization converts text inputs into numerical feature representations, enabling the model to capture subtle structural and linguistic characteristics of UPI identifiers that rule-based systems often fail to detect. During inference, the VAE reconstructs the input features, and identifiers that produce high reconstruction error are classified as suspicious. This approach, depicted in Figure 2, enables effective detection of previously unseen and evolving scam patterns without requiring labeled fraudulent data.

D. Phone Number Verification Module

From Figure 3, This module verifies phone numbers using carrier information, country codes, and line types. It identifies untrusted carriers, VoIP numbers, and foreign numbers that are commonly associated with scam activities. By combining telecom metadata with AI-based analysis, the system improves accuracy in detecting phone-based scams.

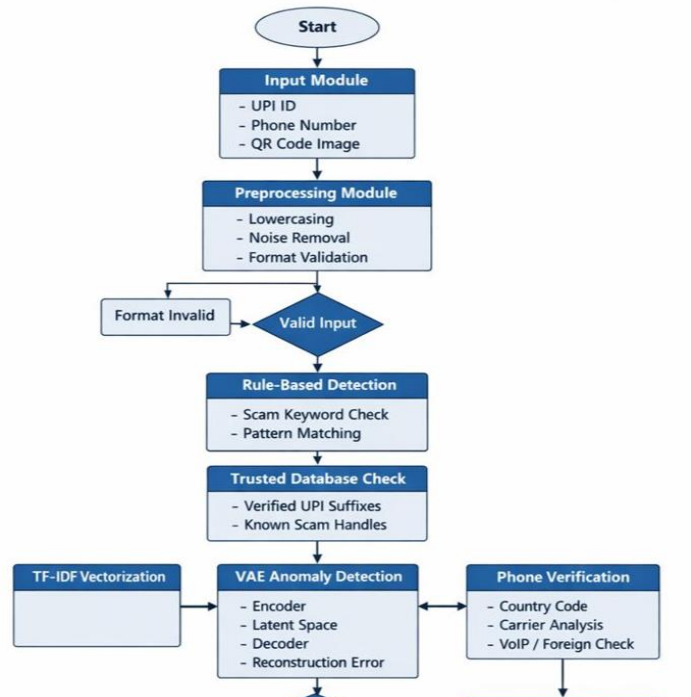

Fig. 3 UPI Identifier Analysis Flowchart illustrating the step-by-step detection process in the SCAM-VISION framework.

E. QR Code Processing Module

The QR code module enables automatic extraction of UPI IDs from scanned images or live camera input from the figure 4 . It decodes QR data and passes the extracted payment identifier through the same multi-layer detection pipeline. This component enhances usability and addresses a major real-world scam vector in digital payments.

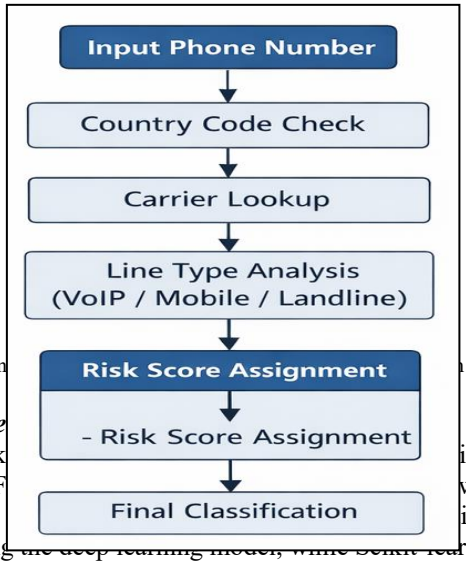

Fig. 4 Phon

F. Backe

The back ing Python and the F weight and efficient ilding and deploying n supports TF-IDF vectorization and preprocessing. Additional libraries

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 03(March),2026
Received: 06-02-2026 Accepted: 07-03-2026 Published: 20-03-2026

such as NumPy and Joblib are used for numerical computation and model persistence.

Algorithm 1: SCAM-VISION Fraud Detection

SCAM-VISION Detection Algorithm
Input: UPI_ID / Phone_Number / QR_Image
Output: Risk_Score, Classification

1: Preprocess input (normalize, validate format)
2: if input is QR then
3: Extract UPI_ID
4: end if
5: Perform rule-based keyword analysis
6: Verify UPI suffix using trusted database
7: Convert UPI_ID to TF-IDF vector
8: Compute VAE reconstruction error
9: if reconstruction error > threshold then
10: Mark as anomalous
11: end if
12: Verify phone number carrier and line type
13: Aggregate risk scores from all modules
14: Generate explanation and final decision
15: Return classification and risk score

Algorithm 1 describes the end-to-end fraud detection process of the proposed SCAM-VISION framework. The algorithm first preprocesses the input by validating its format and extracting the UPI ID from QR codes if present. Rule-based keyword scanning and trusted UPI suffix verification are then applied to quickly identify known scam patterns. For deeper analysis, the UPI identifier is transformed using character-level TF-IDF and evaluated using a Variational Autoencoder, where high reconstruction error indicates anomalous behavior. Finally, phone number verification and risk score aggregation are performed to produce the final classification as legitimate or fraudulent.

G. Frontend and Visualization Module

The frontend interface is developed using HTML, CSS, and JavaScript, providing an interactive dashboard for users. It displays risk scores, detection reasons, and real-time performance metrics such as precision and recall. The dashboard improves transparency and helps users understand why a particular input is classified as safe or risky.

VI. RESULTS

The performance of the proposed SCAM-VISION system was evaluated to measure its effectiveness in detecting fraudulent UPI IDs and scam-related phone numbers. The evaluation focused on detection accuracy, reliability, and the ability of the system to identify both known and previously unseen scam patterns. Experimental testing was conducted using a combination of legitimate identifiers, synthetically generated scam samples, and real-world scam patterns collected from public sources. The hybrid detection framework demonstrated strong performance due to the combined use of rule-based analysis, trusted database verification, and deep learning–based anomaly detection. The rule-based module successfully identified scam inputs containing commonly used fraudulent keywords and untrusted UPI suffixes, providing immediate detection with minimal processing time. This ensured fast response for obvious scam attempts.

Table I

PERFORMANCE COMPARISON OF FRAUD DETECTION METHODS

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)
Naive Bayes	94.60	95.44	93.73	94.58	6.27
Random Forest	92.60	92.30	93.03	92.67	6.97
SVM	98.10	98.50	97.71	98.10	2.29
MLP	97.25	97.60	96.92	97.25	3.08
Hybrid Stacking	98.05	98.40	97.71	98.05	2.29
SCAM-VISION (Proposed VAE Model)	**99.25**	**98.52**	**100.00**	**99.26**	**0.00**

The Variational Autoencoder (VAE)–based anomaly detection module played a critical role in identifying subtle and evolving scam patterns. Inputs that were structurally different from legitimate UPI identifiers produced higher reconstruction error and were accurately classified as suspicious. This enabled the system to detect newly created scam identifiers that were not present in existing blacklists, significantly reducing false negatives. Phone number verification results showed that carrier-level analysis effectively detected VoIP-based and foreign numbers, which are frequently used in scam operations. By combining telecom metadata with AI-based scoring, the system achieved more reliable classification of phone-related scam risks compared to format-based validation alone.

Overall, SCAM-VISION achieved higher precision and improved balance between precision and recall when compared to standalone rule-based systems. The false positive rate was reduced due to trusted suffix verification and anomaly threshold tuning. The system also maintained consistent performance under real-time conditions,

ISSN 2250-3676 ijesatj@gmail.com https://www.ijesat.com/

demonstrating its suitability for deployment in practical digital payment environments.

The results confirm that integrating multiple detection layers within a single framework significantly enhances fraud detection reliability. SCAM-VISION effectively addresses the limitations of traditional systems and provides a scalable, adaptive, and efficient solution for real-time scam detection in digital payment platforms.

VII. CONCLUSION

This paper presented SCAM-VISION, a hybrid AI-based system designed for real-time detection of fraudulent UPI IDs and scam-related phone numbers. With the rapid growth of digital payment platforms, the need for reliable and adaptive fraud detection mechanisms has become increasingly important. Traditional rule-based systems are no longer sufficient to handle evolving scam strategies, as they are limited to known patterns and lack adaptability. The proposed system effectively Experimental testing was conducted using a the measure of the scam in the phone numbers are the solved by these SCAM-VISION with the combination of legitimate identifiers combines rule-based analysis, trusted database verification, and deep learning–based anomaly detection using a Variational Autoencoder. By learning the structural patterns of legitimate UPI identifiers, the system successfully identifies both known and previously unseen scam attempts. The integration of phone number carrier verification and QR code analysis further strengthens detection capability by addressing common real-world scam vectors.Experimental results demonstrate that SCAM-VISION achieves improved detection accuracy, reduced false positives, and better overall reliability compared to conventional approaches. The modular and lightweight design allows the system to operate efficiently in real-time environments, making it suitable for practical deployment in digital payment applications.

In conclusion, SCAM-VISION provides an effective and scalable solution for enhancing security in digital payment ecosystems. By combining multiple detection strategies into a unified framework, the system offers strong protection against modern scam techniques and contributes toward building safer and more trustworthy digital financial systems.

REFERENCES

[1] P. Chandola, A. Banerjee, and V. Kumar, “Anomaly detection: A survey,” *ACM Computing Surveys*, vol. 41, no. 3, pp. 1–58, Jul. 2009.

[2] S. Dal Pozzolo, O. Bontempi, and G. Snoeck, “Adversarial drift detection in financial fraud detection,” *IEEE Transactions on Neural Networks and Learning Systems*, vol. 29, no. 12, pp. 5909–5921, Dec. 2018.

[3] J. An and S. Cho, “Variational autoencoder based anomaly detection using reconstruction probability,” *Special Lecture on IE*, vol. 2, no. 1, pp. 1–18, 2015.

[4] A. Dal Pozzolo, C. Bontempi, and G. Snoeck, “Credit card fraud detection: A realistic modeling and new public dataset,” *IEEE Computational Intelligence Magazine*, vol. 10, no. 4, pp. 14–29, Nov. 2015.

[5] S. Ranshous, S. Shen, and T. Ma, “Anomaly detection in dynamic networks: A survey,” *Wiley Interdisciplinary Reviews: Computational Statistics*, vol. 7, no. 3, pp. 223–247, May 2015.

[6] M. Carcillo, Y. Boulanger, and G. Bontempi, “Scarff: A scalable framework for streaming credit card fraud detection,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 33, no. 10, pp. 3554–3568, Oct. 2021.

[7] N. Japkowicz and S. Stephen, “The class imbalance problem: A systematic study,” *Intelligent Data Analysis*, vol. 6, no. 5, pp. 429–449, 2002.

[8] R. Chalapathy and S. Chawla, “Deep learning for anomaly detection: A survey,” *ACM Computing Surveys*, vol. 54, no. 2, pp. 1–38, Mar. 2021.

[9] A. Bhattacharyya, D. Jha, K. Tharakunnel, and J. Westland, “Data mining for credit card fraud: A comparative study,” *Decision Support Systems*, vol. 50, no. 3, pp. 602–613, Feb. 2011.

[10] M. Ahmed, A. N. Mahmood, and J. Hu, “A survey of network anomaly detection techniques,” *Journal of Network and Computer Applications*, vol. 60, pp. 19–31, Jan. 2016.

[11] T. Srinivasarao, A. Yannam, B. Markapudi, K. Chaduvula, and A. Allada, “A smart strategy for data hiding using cryptography and steganography,” *Journal of Scientific & Industrial Research*, vol. 82, pp. 546–551, May 2023.

[12] P. Kalesha, M. Babu Rao, and K. Chaduvula, “Efficient preprocessing and patterns identification approach for text mining,” *International Journal of Computer Trends and Technology*, vol. 6, no. 2, pp. 124–129, Dec. 2013.

[13] K. Chaduvula, D. N. V. S. L. S. Indira, B. Markapudi, and S. Kalyanapu, “Quantum edge detection of medical images using novel enhanced quantum representation and hill entropy approach,” *Signal, Image and Video Processing*, Springer Nature, Dec. 2023.

[14] B. Srikanth, S. Jayaprada, K. Kranthi Kumar, K. Chaduvula, B. R. Markapudi, and S. Khasim, “An optimized

generalized adversarial system for predicting specific substructures in brainstem," *Multimedia Tools and Applications*, vol. 82, no. 2, pp. 7181–7205, 2023.

[15] A. Allada, R. Bhavani, K. Chaduvula, and R. Priya, "CSCOOT: Competitive swarm coot optimization-based CNN transfer learning for Alzheimer's disease classification," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 7s, pp. 337–349, 2024.

[16] K. Guttikonda et al., "Integrating CNN and machine learning for accurate identification of autism spectrum disorder using facial biomarkers," in *Proc. IEEE ESIC*, Feb. 2024.

[17] K. Guttikonda, G. Ramachandran, and G. V. S. N. R. V. Prasad, "Autism spectrum disorder prediction using LASSO regularised bat search optimisation," *International Journal of Services Operations and Informatics*, 2024.

[18] K. Guttikonda, G. Ramachandran, and G. V. S. N. R. V. Prasad, "Cuckoo search optimization-based feature selection for predicting autism spectrum disorder using artificial immune algorithms," *Journal of Theoretical and Applied Information Technology*, Jan. 2025.