Journal of Advances in Management, Engineering and Science (JAMES), July 2026; 1(3): 23-36

Research Article

Hybrid Machine Learning Model for UPI QR Code Fraud Detection and Secure Online Payment Authentication

P. Dileep Kumar Reddy, Professor, CSE Department, Narsimha Reddy Engineering College (Autonomous), Secunderabad, Telangana State, India- 500100., *Email:-* dileepreddy503@gmail.com

N Rajasekhar, Professor of CSE & Dean-External Affairs, Narsimha Reddy Engineering College (Autonomous), Hyderaba Email:- rajasekhar.cse@nrcmec.org

Received: 11th May 2026; Accepted: 18th June 2026; Published: 9th July 2026

https://doi.org/10.65470/james.v1i03.34

Abstract – *With the rise of Unified Payments Interface (UPI), QR code-based payments and digital banking services, the online payment scenario has undergone a sea change, making monetary transactions fast, simple and cashless. However, digital transformation has also fuelled cyber frauds such as fake QR codes, phishing, identity theft, account takeovers, social engineering and payment frauds. Current fraud detection methods usually rely on fixed rule-based systems that cannot adapt to changing fraud trends and often generate high false positive rates, thereby impacting transaction safety and user experience. To address these issues, this paper proposes a Hybrid Machine Learning Model for UPI QR Code Fraud Detection and Secure Online Payment Authentication by combining Convolutional Neural Networks (CNN), Bidirectional Long Short-Term Memory (BiLSTM) and Extreme Gradient Boosting (XGBoost). The proposed framework uses extensive information pre-processing, feature engineering and feature selection techniques for improving the quality of transaction data before classification. CNN is used to extract transaction features. BiLSTM is used to capture sequential behavioural patterns and temporal dependencies. Deep feature representations are fused to classify fraud accurately by XGBoost. The system also has an adaptive multi-factor authentication mechanism based on the predicted fraud probability, which involves OTP verification, biometric authentication, PIN validation and trusted device verification to improve the security of the transaction. Experimental results show that the proposed hybrid model outperforms traditional machine learning and deep learning models on multiple evaluation metrics, including Balanced Accuracy, Matthews Correlation Coefficient (MCC), Cohen's Kappa Score, Log Loss and Average Precision (AP). The results validate the proposed approach to improve the accuracy of fraud detection, reduce false alarms, increase the reliability of authentication and provide a scalable, intelligent and secure framework to protect UPI QR code transactions from evolving cyber risks. The proposed system combines advanced artificial intelligence techniques and adaptive security mechanisms for real-time fraud detection to build a reliable digital payment ecosystem.*

Keywords— *Unified Payment Interface (UPI), QR code Fraud detection, Hybrid ML Learning, Convolutional Neural Network (CNN), BiLSTM, XGBoost, CatBoost, Digital Payment Security, cybersecurity, Authentication of multi layers, Explainable Artificial Intelligence*

INTRODUCTION

Nowadays, wherever the people travel or stay the digitalisation has equipped and this cannot be removed, in this the payment systems have largely taken place in the digitalization, and it has also transformed the way individuals and business conduct the financial transactions. Among the several payment methods the Unified Payment Interface (UPI) has emerged as one of the most popular real time Payment platforms due to its speed, convenience, and the ease of the study. The widespread use of the QR based payments in the stores, online shopping, restaurants, health care, transportations, and all other sectors. As the smartphones and the Internet connections continue to expand and better the QR codes has become a common way of the usage. Apart from the advantages the usage of the QR Code has become the way for the cybercriminals for making the fraud. The most common frauds are like the fake QR Codes, QR Code replacement activities, phishing, social engineering. In many cases the people by mistake scan the wrong QR Code that redirects into the frauds, these leads to several changes like the money will also be lost and the trust on the online payments also lasts. The traditional methods work on the detective systems that searches for any new malicious attack patterns, because all those methods only depend on the predefined algorithms, calculations and the static thresholds. For this problem the Machine Learning has become one of the promising solutions for the financial fraud detection, prediction and analyse the hidden data, and also by learning from the historical data the dataset becomes more powerful and performs well, but using the dingle model in the ML is not useful because it may affect through the reduced performance, overfitting, positive rates, and the reduced performance. So, the implementation of the Hybrid Machine Learning always benefits the most by removing all the difficulties and giving support for the long term also. This research proposes the Hybrid Machine Learning model for the UPI QR code fraud detection. The architecture and the implementation should be proper and efficient so that the whole system enables the best method for the human friendly and fraud disabled method (1). The demonetizations and the outlines in the architecture, operational framework, advantages and the implementations challenge are not taken care and without security anything is not good for current trends (2). The UPI payment usually is hacked because everyone depends on the money, each second crores together transactions are happening by which the people are dependent and the lives are also disturbed so the live example is shown (3). The Plastic money refers to the debit card or the credit card that should be carried and the PIN should be privately maintained and if the card mises then issues may happen and some people keeps the PIN number in the wallet of that car by which others can easily get and do the transactions so to avoid all these the UPI was introduced but this also has some limitations (4). The investigation of the User Experience (UX) is generalized, and the usage of the Cross Tabulation method is used to find the usage of the online payment and the fraud detected are analyse and said that the more cases are observed (5). Several online payments are there like Unified Payments Interface (UPI), Mobile banking, Digital wallets, Immediate Payment Services (IMPS), National Electronic Fund transfer (NEFT), Real Time Gross Settlement (RTGS), Bharath Interface for Money (BHIM), unstructured Supplementary Service Data (USSD), Buy Now Pay Later (BNPL) in all these the Government or private is handling securely but still the frauds are going on, but in nowadays the percentage of frauds in the bar code has increased so to decrease that the model should be implemented (6). The data can be saved using the blockchain and the Graph Attention Network, but these are the traditional methods that will not support the large data so the new methodology should be implemented (7). The QR (Quick Response) contains the series of the black and the white squares that can be read by the machines that stores the websites of the particular payment that redirects once the bar code is scanned this is taken as advantage and used by the hackers to encrypt the codes and make the payment fraud and betray the common people (8). According to the point Of Sales (POS) the transactions should be accepted by the merchant side that contains the separate code is assigned that should work properly and supports every payment, there are two types of the QR codes one is static that don't require the extra website confirmation but the second one which is the dynamic one changes with the time wants the immediate response and correct flow this will be riskier if the server and the flow is not maintained properly, to perform this the strong method should be implemented so that no further issues happens (9). The QR code provides the low cost and the infrastructure-based implementation, and the Resource Based View (RBV) and the Technology Acceptance Model (TAM) are integrated for the better performance but lacks in the proper maintenance (10).

RELATED WORKS

The Key challenges include the ephemeral evidence, encrypted and proprietary ecosystems, weak end point hygiene, gaps in logging KYC, these will affect the safe transfer of the money and rises to the fraud under the real time situation (11). The confidentiality, transaction

nonrepudiation management, Authentication of the Identity of the customers, Data and transaction integrity, Access and availability, Privacy of the customer information these are the six main properties are used to evaluate the bank transaction and improve the quality and security but not implemented the ML (12). The UPI works on the Standard API (Application Programming Interface) that verifies the Aadhaar details and gets connected to the payment gateway and this process should be conducted with all assets ready so that the whole process is observed and verified (13). The different challenges are as follows Data fragmentation, Encrypted and provenance gaps, Devica and the user privacy, Money mule networks and rapid cashouts, QR generation and maintenance these should be taken care and find a solution to avoid the frauds and thefts (14). In the Diffusion of the innovation Theory the usage of the new models based on the Machine Learning and the arrival of the deep learning helps to remove the challenges faced during the transactions and the payments (15). The digital era faces many challenges during the usage of the digital things it may be payments or websites or the applications but due to the lack of awareness the people are not knowing the measurable things and precautions about how to use and why we need to use this also matters to reduce the frauds, since people knows the whole procedure, no one can do the fraud (16). The Machine Learning has implemented in the fraud detection and the findings found that only implementing the single method does not give the best approach instead the combination or a hybrid model should be presented so that all the challenges can be removed (17). The Artificial Neural Network is used to find the fraud detection for the credit card; this methodology works better compared to others but cannot be implemented in the further since this is not the stable format of doing (18). The Rule Based Model is introduced by which the machine learning is implemented and compared with the existing methods but did not find the solution exactly but this method can be implemented for the current scenario short time not insisted for the long term (19). The Machine learning integration is done that uses the Support Vector Machine (SVM) and the KNN (K-Nearest Neighbours), Random Forest, Boosting and the Bagging but becomes unstable for the large data (20). To secure the QR code the precautionary measures are told but the exact method is not implemented by which that can be used for the real time and this may affect the implementations of the other software that are required for the security purposes (21). The method gives the hybrid CNN, and the Random Forest gives the solution to the existing problem, but this gives the immediate solution, but this may not last for the long term and may cause defects of missing data (22). To find the fraud and the threat the Firebase collections that are blacklisted upi, risk patterns, ML models help the system store and retrieve fraud data efficiency (23). The novel modelling BiLSTM and the transformer-based encoders can be the best approach for the machine learning by which the method can show the performance but the pattern does not suite for the several UPI bar codes so the additional support is required so that the machine learning approach will be best and implemented (24). The Multi factor Authentication is required for the proper process, and the mechanism should be implemented and followed correctly through the entire process of security and the management, this small part can be implemented by which the entire process can be stable for the whole time (25). To detect the illegal content utilising Score card (SC) duplication, the Improved Swarm Optimization (ISO), is introduced this can be implemented before releasing the code, this novel method helps in the finding the correct way (26). Cybersecurity concerns and usage should be taken care since the cases of the frauds are increasing so the Denial of Service (DoS), and the Distributed Denial of Service (DDoS) are instructed and maintained correctly and while integration it into the ensemble method the steps should be followed correctly (27). The SVM and the Multi-Layer Perceptron (MLP), and AdaBoost and the Matthews Correlation Coefficient (MCC) can be implemented and the results of this gives the best approach since this can be used as the vital approach in the security concerns (28). The Network Intrusion Detection System (NIDS) is integrated in the Machine Learning so that the system gets support and the mechanism flows correctly with the smooth flow and this implementation will be secure and efficient (29). The Industrial Internet of Things has enabled the sensing and identifying the threats as soon as possible and then integration of the hybrid model helps for the further process that makes the system better compared to others (30).

METHODLOGY

The proposed framework starts with the customer initiating the payment, using the Unified Payments Interface (UPI)- enabled mobile transaction. UPI was developed by the National Payments Corporation of India (NPCI) which is a real time payment method that allow the users to transfer the funds from one account to another, with the increasing popularity of the QR based transaction, which is easier and faster to use. During the payment the data is collected, and the real process starts here the data will be cleaned, normalized and the missing values are replaced all this is done using the data preprocessing step then the Feature engineering is done where the feature selection and the extraction happens by which the required and efficient features are grouped and moved to the next steps so that the huge data should not bother the further

process then the Feature vector generator will generate the transaction features for the further proceedings, then the Hybrid Machine Learning is employed where the whole system performance depends here the CNN i.e. Convolution Neural Network is applied for the feature extraction, then the BiLSTM i.e. Bi-directional Long Short Term Memory is employed so that the sequential learning pattern is followed and the memory should be stored for the long-term usage so the preferred method is the BiLSTM can be used for better process, and the XGBoost for the final classification since this enables the machine learning approach and the stability is confirmed and process the large data easily and efficiently so these are the main methods that helps to process the data of the bar code and the customer details, then the Fraud probability calculation is done which acts like the cybersecurity layer that detects the fraud percentage by analysing different characters and the parameters and utilizing the previous data for reference and the threshold is also predefined using the prior calculations now the Risk core will be generated then it is compared with the Threshold here the process has two conditions if the risk score is greater than the threshold then it will be sent to multifactor authentication to detect the fraud and this is more powerful step, if the Risk factor is less than the threshold then this will be sent to the Secure Authentication that will only sees whether the PIN is correct and the device then is it ok then the authentication step is completed if this authentication is successful then the process approves the transaction and the final step is executed otherwise if unusual activities or the fraud is found then immediately the whole transaction is blocked and this will be noted in the database and the adaptive model learning is done to increase the efficiency and the stability and the transparency of the whole system, this is the better approach for preventing the fraud using the bar code of the online payments.

A. Initiation of the UPI QR Code Payment:

In this method the user first opens the Mobile applications like PhonePe or Google pay or the Amazon pay and selects the payment method after the camera activates then the scanning of QR code is done this bar code contains the parameters like Virtual Payment Adress (VPA), merchant identification number, merchant name and the acquiring bank information, transaction currency, transaction amount that is fixed by the user, and additional codes. These information helps in the routing of the payment, after the transaction happens during this process the system also notes some important features like the Operating system version, Type of network, application version, IP address, SIM card information, and the time stamp, fingerprint. This helps to analyse the behavioural consistency and the further proceedings. The transaction information that is stored in the sequential format that is represented as in Eq (1) as follows:

$$T_d = \{D_1, D_2, \dots\dots\dots\dots..D_n\} \quad (1)$$

During this process the proposed method also takes care of the security measured during the initial transaction and the scanning process. Then the data is processed to the next step.

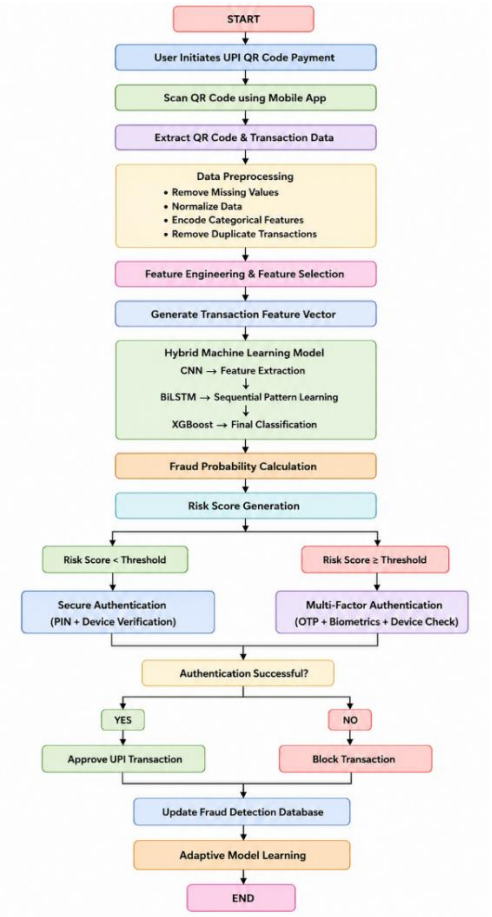

Fig 1. Flowchart of the proposed model

The Figure 1 represents the whole flowchart that acts like the blueprint of the proposed hybrid model for the fraud detection.

B. QR Code Payment:

The QR (Quick Response) code has become one of the primary medium for the UPI based payment because this enables the fast, contactless, and the user-friendly transactions without requiring the manual payment method. This QR Code is the two-dimensional barcode can store the information like MA, VPA, amount and the transaction details. Although this payment method has the tight security but still lacks some security that leads to the fraud or scams so to avoid such scams the proposed model introduces the new ensemble method.

Then the QR decoding process starts that converts the graphical QR Code into the machine-readable information, during this all the data is stored in the structured format, the decoded transaction is always stored in the set for the further proceedings as shown in the Eq (2) as follows:

$$Q_d = \{q_1, q_2, q_3, \dots \dots \dots q_n\} \quad (2)$$

The framework also stores the contextual transaction information that will not be directly stored in the QR Code, so this data is represented as in Eq (3) as follows:

$$T_d = \{t_1, t_2, \dots \dots \dots \dots t_n\} \quad (3)$$

To further increase the transaction security the proposed method calculates the Preliminary QR code authenticity score based on the multiple validation parameters. The authenticator score is calculated as given in Eq (4) as follows:

$$Q_S = \sum_{i=1}^{n} w_i \times q_i \quad (4)$$

Where the Q_S represents the QR authenticator score, q_i denoted the value of the i^{th} QR verification parameter and the n denote the total number of the verification parameters. The higher authenticity score indicates the greater confidence of the scanned QR code is genuine, lower score tells the fraud detection and requires the security measures.

C. *Pre-processing of the data:*

The data processing is the crucial step, and the pre-processing is critical step and this should be followed correctly, and the steps are followed for the proper usage. The dataset is obtained from the open source Kaggle (31) for the testing and proving this method in the real time the data is directly connected to this method, so here the data usually will be in the raw format and this should be converted into the structured format, this includes the missing value handling, duplicate removals, Noise removals, outlier detection, Data encoding, Feature Normalization.

1. *Missing Value Handling:*

The missing values are commonly present in the data that happens due to the transaction logs, severe synchronization, data collection errors. Missing information may occur in the transaction amount, merchant information, account balance attributes. For these the data are replaced using the Eq (5) as follows:

$$\bar{M} = \frac{1}{N} \sum_{i=1}^{N} M_i \quad (5)$$

Where the $\bar{M}$ is the Mean value, M_i is the Individual feature value, and N is the total number of observations.

2. *Duplicates removal:*

The duplicates are always disturbing the whole data so the removal of these are very important, to do this the framework compares the transaction identifiers like the transactions, timestamps, MerchantID, SenderID, recieverID here only the one entity is choosed at final. This is mentioned as follows in the Eq (6) as follows:

$$Hash(t_i) = Hash(T_j) \quad (6)$$

Where the T_i represents the transaction of i and T_j represents the transaction of j if both the hash values are identical the two records are considered as duplicates.

3. *Noise removal:*

The noise will be everywhere if this is not removed then the entire process may affect and gives the wrong implementation, so this is identified using the noise filtering techniques for example the transactions that contains the negative amount values, invalid timestamps, corrupted merchant identifiers, or the unrealistic account balances. By enabling the noise filtering all these data's can be removed and ready for the next procedure.

4. *Outlier detection:*

The fraud always happens in the abnormal behaviours, so this is considered as the main issue and correctly observed and figure it out. The proposed model uses the Z-score computation for identifying the extreme outliers as given in the Eq (7) as follows:

$$Z = \frac{x - \mu}{\sigma} \quad (7)$$

Where the Z represents the Final output after removal of the noise and the X is the current feature value, μ is the Mean value, σ is the standard deviation but always whatever the method used that should be rechecked and validated finally so the transactions having the extremely high Z Score values are examined further, this will improve the correctness and the stability of the model.

5. *SMOTE for handling the classes:*

The Synthetic Minority Over Sampling Technique (SMOTE) generates the synthetic fraud samples by interpolating between the neighbouring minority class observations instead of simply duplicating the existing

fraud records. The synthetic sample is generated as given in the Eq (8) as follows:

$$D_{new} = D_i + \emptyset(D_{NN} - D_i) \quad (8)$$

Where the Minority class is represented as the D_i, nearest neighbour minority sample is denoted as D_{NN}, and the $\emptyset$ represents the random values between 0 and 1.

D. Feature Engineering and Feature Selection:

The Feature Engineering is one of the most significant stages in the proposed machine learning model because the effectiveness of the fraud detection depends not only on the learning the algorithm depends on the quality and quantity. The Raw transaction data contains the following after the preprocessing transaction amount, merchant ID, sender account, receiver amount, transaction timestamp, QR Code details.

1. Transaction amount Risk Score:

The transaction amount is one of the strongest indicators of the fraudulent activity. Fraudsters often attempt to transfer unusually transfer unusually high amounts, repeatedly transfer the less amount, the transaction amount risk score is calculated as given in the Eq (9) as follows:

$$T_{rs} = \frac{A}{M_t} \quad (9)$$

Where the A represents the Amount that gives the current payment value, and the maximum amount transaction is represented as M_t. Transactions with the larger normalized values receives higher preliminary risk levels.

2. Transaction Velocity:

Frauds always make the multiple transaction at a particular period so this can be recognized and found the thefts, so the transaction frequency becomes very important, the transaction velocity is defined as following Eq (10),

$$T_V = \frac{N}{\Delta T} \quad (10)$$

where the N is the number of transactions, ΔT is the time interval.

3. Merchant Trust Score:

The merchants always different from heavy historical data to newly started business data, so the merchant trust score is calculated as given in Eq (11) as follows:

$$M_{ts} = \frac{S_t}{T_t} \quad (11)$$

Where the S_t represents the Successful transactions, T_t is the Total transaction.

4. QR Code Authenticity Score:

This is the main phase where the whole model will give the flexibility and stability and the fake QR are mentioned and can be easily found. The QR Code Authenticity Score is given in Eq (12) as follows:

$$Q_{as} = \sum_{i=1}^{n} w_i q_i \quad (12)$$

Where the q_i is the QR verification parameter, w_i is the corresponding importance weight. The Parameters include the Merchant verification, QR format verification, Payment Adress verification, Merchant Registration Status, Transaction Reference Validation and the QR Code Age. A higher authenticity indicates the greater confidence that the QR code is genuine.

5. Authentication Strength Score:

The whole method needs the online interactions, and requires the online payment authentication, several authentications provide different levels of the security. The Authentication Strength score is represented as given in Eq (13) as follows:

$$A = \sum_{i=1}^{m} A_i \quad (13)$$

Where the authentication factors include like the PIN verification, OTP Verification, Biometric Authentication, Device Authentication, Face recognition. Transactions with the stronger authentication receive the lower fraud probabilities.

E. Feature Vector Generation:

After generating all the engineered features, they are combined with the original transaction attributes to create the final feature vector. The feature vector is represented as given in the Eq (14) as follows:

$$F_v = \{F_1, F_2, \ldots\ldots\ldots\ldots F_n\} \quad (14)$$

Where the features include like Transaction amount, Merchant Trust Score, Transaction Velocity, Device Consistency, Location Consistency, QR Authenticity Score, Authentication Score, User Behavioural Score, Transaction Time Stamp and the Fraud label.

F. Feature Selection:

This is the method that gives the more better parameter since the future method always need the best parameter and this needs the more relevant data in this method the structured and the better feature that is required will be taken and sent into the next step. The feature Importance Score is computed as given in the Eq (15) as follows:

$$F_{ij} = \sum_{k=1}^{m} Gain_{jk} \quad (15)$$

Where the F_{ij} is the Importance score of j, $Gain_{jk}$ is the information gain contributed by feature j at split k, m is the number of decision trees.

G. Hybrid CNN-BiLSTM-XGBoost Model for the UPI QR Code:

This is the main and important step that is used for the fraud detection and this is the core component that integrates the Convolution Neural Network, Bidirectional Long-short Term Memory, and the Extreme Gradient Boosting to accurately detect the fraudulent UPI QR Code transactions and ensuring the proper online transaction. The Machine Learning Algorithms such as the Decision Trees, Support Vector Machine, perform well on the structured data, but fails to capture the complex relationships. So the mathematical representation of the whole model is represented as given in Eq (16) as follows:

$$P_{tc} = XGBoost\left(BiLSTM\left(CNN(F)\right)\right) \quad (16)$$

Where the P_{tc} is the predicted transaction class, CNN(F) is the extraction of the local transaction features, BiLSTM () is the learning of the sequential behavioural patterns, XGBoost () performs the final fraud classification.

1. Convolution Neural Network:

The Convolution Neural Network is the first method is used for the whole model, this is mainly used for extracting the important and the effective features for the structured financial transactions, the convolution operation is mathematically represented as given in the Eq (17) as follows:

$$C_o = \sum_{i=1}^{m} F(i+k) \times W(k) + b \quad (17)$$

Where the C_o is the Convolution output, $F(i)$ is the input feature vector, W(k) is the Convolution filter weights, b is the bias and the m is the filter size. After the convolution, the Rectified Linear Unit (ReLU) activation function introduces the non-linearity into the learning process. The activation function is given by the Eq (18) as follows:

$$ReLU(x) = \max(0, x) \quad (18)$$

Where this will evaluate the results by removing the negative values and preserving the positive values. Then the pooling operation is represented as given in the Eq (19) as follows:

$$P = \max(C) \quad (19)$$

Where the P denotes the pooled feature map, this pool reduces the computational complexity, minimizes the redundant information, and improves the robustness of the fraud detection model against the noisy transaction data. At last the pooled feature maps are flattened into a one-dimensional feature vector, this is given in the Eq (20) as follows:

$$FV_{cnn} = Flatten\ (p) \quad (21)$$

The resulting feature vector represents the high-level transaction characteristics extracted by the CNN and is then forwarded to the BiLSTM for sequential Learning.

2. BiLSTM:

The CNN provides the features that are nice but to handle the high-level transaction data the better model is required. The frauds usually follow a pattern that will be executed in the sequential format, but the CNN cannot be able to recognise this, so the Bidirectional Long-short term memory that recognises these features. Long Short-Term Memory (LSTM) is a type of the Recurrent Neural Network (RNN) architecture that is designed to overcome the vanishing gradient problem. The bidirectional will help to the predict the more absolute and feature that gives the whole model better stability.

In this model the CNN generated features are sequentially arranged then pass this to the BiLSTM network. Each sequence contains the transaction characteristics, authentication strength, transaction velocity, and the user behavioural score. The BiLSTM analyses the sequential observations to determine whether the current transaction deviates from the customers normal payment behaviour. The input gate evaluates the importance of the newly arriving transaction features before updating the internal memory as given in the Eq (22) as follows:

$$i_t = \sigma(w_i x_t + u_i h_{t-1} + b_i \quad (22)$$

Where the i_t is the input gate activation, x_t is the current transaction feature vector, $h_{t-1}$is the previous hidden state, w_i is the input weight matrix, U_i is the recurrent weight matrix and the b_i is the bias vector, and the σ is the sigmoid activation function. The sigmoid function gives the value between 0 and 1 allowing the network to decide how much the new transaction information should enter the memory cell.

The forget gate removes the unnecessary information from the memory cell while retaining the important behavioural characteristics. The forget gate is computed as given in the Eq (23) as follows:

$$F_t = \sigma\left(w_f x_t + U_f h_{t-1} + b_f\right) \quad (23)$$

Where the F_t is the Forget gate activation, w_f is the weight matrix and the U_f is the Recurrent Weight Matrix, and the b_f is the bias.

The Candidate Memory Stage generates the new transaction knowledge that may be incorporated into the memory cell it is calculated as follows in the Eq (24)

$$\bar{c_t} = \tanh(w_c x_t + U_c h_{t-1} + b \quad (24)$$

Where the $\bar{c_t}$ is the candidate memory, w_c is the weight matrix, U_c is the recurrent weight matrix, b is the bias.

The memory cell combines the previously stored information with the newly generated transaction knowledge. The updated memory state expresses as in the Eq (25) as follows:

$$C_t = f_t \odot c_{t-1} + i_t \odot \grave{c_t} \quad (25)$$

Where the C_t is the Current memory state, c_{t-1} is the previous memory state, $\odot$ is the element wise multiplication.

The output gate determines the information from the updated memory cell should be transmitted to the next processing stage, the output gate is represented as in the Eq (26) as follows:

$$O_t = \sigma(w_o x_t + U_o h_{t-1} + b \quad (26)$$

Where the O_t is the output gate activation, w_o is the weight matrix, U_o is the recurrent weight matrix, b is the bias. The hidden stage generated by the output gate is given in Eq (27) as follows:

$$h_t = O_t \odot \tanh(C_t) \quad (27)$$

The hidden state gives both historical and the current transaction behaviour and becomes the feature representation forwarded to the classifier. Unlike the traditional LSTM the proposed model processes the transaction sequence in both the forward and the backward directions. The forward hidden state is given in the Eq (28), the backward hidden state is given in Eq (29), and the final BiLSTM representation is obtained by the combination of the both the outputs given in the Eq (30) as follows:

$$\overrightarrow{h_t} = LSTM(x_t) \quad (28)$$

$$\overleftarrow{h_t} = LSTM(X_t) \quad (29)$$

$$H_t = [\overrightarrow{h_t}; \overleftarrow{h_t}] \quad (30)$$

Where the $\overrightarrow{h_t}$ is the forward Sequence Information, and the $\overleftarrow{h_t}$ is the Backward Sequence Information. This combined representation captures the complete transaction dependencies across the entire sequence. The final BiLSTM output is represented by the Eq (31) as follows:

$$H = \{h_1, h_2, \ldots\ldots\ldots\ldots h_n\} \quad (31)$$

Where the H denotes the sequence of the learned hidden feature vectors representing the complete transaction history. Then this is forwarded to the next further steps.

3. XGBoost based Fraud classification:

After the two steps of filtering by the CNN and the BiLSTM the data is pushed into this step that is Extreme Gradient Boosting where the final fraud classification happens. Due to its superior learning capability and the robustness against the overfitting. XGBoost constructs the decision tree sequentially where each new tree attempts to correct the prediction errors generated by the previous trees. Also, the nonlinear relationships are captured and classify the fraudulent transactions. This finally classifies the whole data into either one of them i.e. either the Legitimate or Fraudulent. The Prediction function of the XGBoost is given in the Eq (32) as follows:

$$\hat{y_i} = \sum_{k=1}^{k} f_k(x_i) \quad (32)$$

Where the $\hat{y_i}$ is the predicted output of the transaction i , K is the number of decision trees, f_k is the individual decision tree, x_i is the input feature vector generated by the BiLSTM. The final prediction is obtained by combining the decision trees.

To increase the generalization and reduce the overfitting and make the model more stable the objective function is applied that is given in Eq (33) as follows:

$$O_f = \sum_{i=1}^{n} L(y_i, \hat{y_i}) + \sum_{k=1}^{k} \Omega(f_k) \quad (33)$$

Where the $L(y_i, \hat{y_i})$ is the classification loss function, $\Omega(f_k)$ is the regularization function, and n is the number of the training samples. The prediction error is detected by the first component and the penalisation over the complex decision tree is done by the second component. The XGBoost improves the prediction performance by iteratively correcting the previous errors. During each iteration, it follows the Eq (34) as given:

$$P_{new} = P_{old} + L_r \times t \quad (34)$$

Where the P_{new} is the new prediction, P_{old} is the previous prediction, L_r is the Learning Rate and the t represents the decision tree.

The fraud probability is estimated from the computation of the probability that the transaction is fraudulent and the sigmoid function for this is given in the Eq (35) as follows:

$$P_f = \frac{1}{1 + e^{-z}} \quad (35)$$

The higher probability indicates the higher likelihood of the fraud.

Then the transaction classification is done using the logic that means it compares with the predefined threshold like shown in the Eq (36) as follows:

$$Class = \begin{cases} F, & P(F) \geq \theta \\ L, & P(F) < \theta \end{cases} \quad (36)$$

Where the θ is the threshold, F represents the Fraud, and the L represents the Legitimate.

H. Secure Online Payment Authentication:

The challenges of the online payment that is done by using the QR Code should be taken care and this requires the attention of the people and the awareness including the different layers of the authentication, to address the security challenges the proposed framework incorporates the multi factor Authentication (MFA) mechanism that combines the PIN Verification, One Time Password (OTP) verification, biometric authentication, device verification before approving the transaction. The authentication process begins immediately after the hybrid machine learning classifies a transaction as legitimate. Traditional methods use the direct authentication, but the multi-layer authentication and the verification is done, each factor independently verifies a different aspect of the user identity, reducing the financial transactions. If any authentication is failed, then the transaction immediately fails.

1. Personal Identification Number (PIN) Verification:

The first authentication layer verifies the user UPI PIN. This is a numeric code that is only known to the user only, during the process the PIN should be entered by the user, and this is stored by the bank in the encrypted format using the cryptography and the verification process is represented as given in Eq (37) as follows:

$$PIN_s = \begin{cases} 1, Hash(PIN_{input}) = Hash(PIN_{stored}) \\ 0, \quad Otherwise \end{cases} \quad (37)$$

Where the PIN_s is the verification result, PIN_{input} is the PIN entered by the customer, PIN_{stored} is the encrypted PIN stored in the banking database. If both hash values match then only the authentication process continues, otherwise the transaction is terminated.

2. One Time Password (OTP) Verification:

The OTP validation is done, so the OTP is generated automatically by the bank side, since this is valid only for few times the process also remains valid, the OTP verification process is expressed as given in the Eq (38) as follows:

$$OTP_S = \begin{cases} 1, & OTP_e = OTP_g \\ 0, & Otherwise \end{cases} \quad (38)$$

Where the OTP_e is the OTP Entered, OTP_g is the Generated OTP.

To further enhance the ability of the transaction the proposed methodology incorporates the biometric authentication, the biometric similarity is calculates as given in Eq (39) as follows:

$$Similarity = \frac{Match\ score}{Maximum\ score} \quad (39)$$

I. Secure payment Authorization:

When the authentication is completed the banking then the server sends the transfer through the National Payment Corporation of India (NPCI) payment gateway. The amount is securely sent from the bank to the users account, a unique transfer number is generated and stored in the banking database for the further proceedings. During this if the payment limit exceeds or any fraud found immediately the entire process is blocked and stopped.

J. Continuous Fraud Learning:

The transaction is completed or not is the matter but the system always if a payment is initiated immediately all the information is stored so that in the future this can be helpful to know the details and also to find the particular scam or the fraud, this continuous learning helps in the improvement of the model and the findings, the model update process is shown in the Eq (40) as follows:

$$Model_{new} = Train(Model_{old}, New\ data) \quad (40)$$

Continuous learning makes the mechanism more stable and helpful for the final proceedings.

RESULT AND DISCUSSION

The results are evaluated by measuring with any metrics or the method so that the models robustness, stability, time for the performance everything can be calculated and say that the model is appropriate or not so for the proposed model the performance evaluation metrics used are listed below with the formula's.

1. Balanced Accuracy:

The Accuracy measure the average of the sensitivity and specificity, which gives the system to detect the fraud and enhance the quality and proof of the model. It also helps for the classification process. This is given by the Eq (41) as follows:

$$Accuracy = \frac{Sensitivity + Specificity}{2} \quad (41)$$

Where the Sensitivity represents the True positive by the combination of True Positive and False Negative, and specificity represents the True negative by the combination of True negative and the False Positive.

2. *Mathew's Correlation coefficient:*

This method is used mainly to measure the binary classification of the confusion matrix and parameters, so this helps in the dealing of the imbalanced data and the long correlation effects. This is given in the Eq (42) as follows:

$$MCC = \frac{TP \times TN - FP \times FN}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}} \quad (42)$$

3. *Cohens Kappa score:*

This predicts the values between the Actual and the Predicted parameters and this also keeps in mind about the chance of occurrence. Here the higher Kappa values indicate the better model's reliability and the lower values are considered as inappropriate. This is given in the Eq (43) as follows:

$$k = \frac{P_o - P_e}{1 - P_e} \quad (43)$$

Where the P_o is the observed parameter, P_e is the expected parameter by chance.

4. *Binary cross entropy:*

By removing the incorrect and over confident parameters, this evaluates the probability predictions and quality. This value gives the models performance ability. This is given in the Eq (44) as follows:

$$Log_{loss} = \frac{1}{N}\sum_{i=1}^{N}[y_i \log(P_i) + (1 - y_i)\log(1 - P_i)] \quad (44)$$

5. *Average Precision:*

This method is used to convert the precision recall curve into a single value and it used to find the highly imbalanced fraud databases and the relationships. The higher value indicates the better identification of the frauds.

$$A_p = \sum_{N}(R_n - R_{n-1})\,P_n \quad (45)$$

Where the A_p is the Average precision, P_n indicates the precision at threshold N and the R_n is the recall at the threshold N.

TABLE I. PERFORMANCE COMPARISION OF FRAUD DETECTION MODELS

MODEL	BA (%)	MCC	KS	Log Loss	AP (%)
Logistic Regression	83.42	0.792	0.785	0.462	84.18
Decision Tree	85.76	0.824	0.816	0.396	86.41
Random Forest	87.95	0.851	0.844	0.341	88.62
CNN	89.84	0.879	0.871	0.287	90.33
BiLSTM	91.28	0.901	0.895	0.241	91.87
CNN & RF	92.63	0.924	0.918	0.194	93.08
Proposed Hybrid model	94.36	0.944	0.946	0.128	94.82

The Table I represents the comparison of the proposed model with the other models that give the clear picture about the prediction of the frauds.

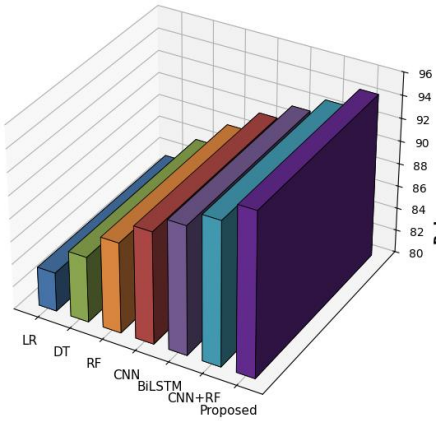

Fig. 2 Comparison of Prediction Results

The three models in the figure 2 gives the comparison of the proposed model with the existing one.

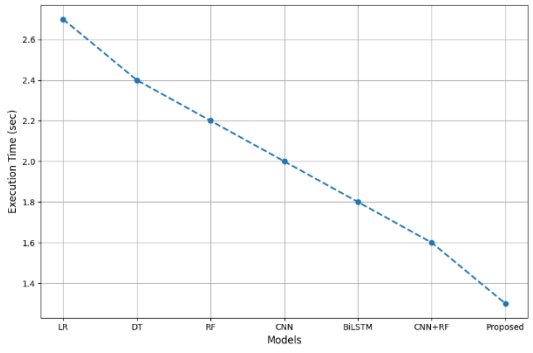

Fig 3. The Execution time of the models

Graph 3 gives the Execution time of all the models by which the model to be selected in critical situation can be identified easily

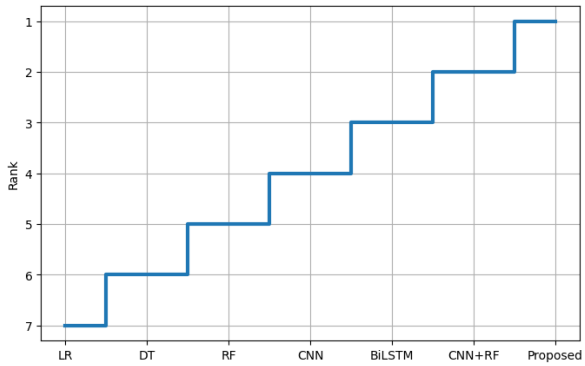

Fig 4. The Ranking graph

Figure 4 shows the ranking of the proposed model in the fraud detection according to the survey done by NPIC.

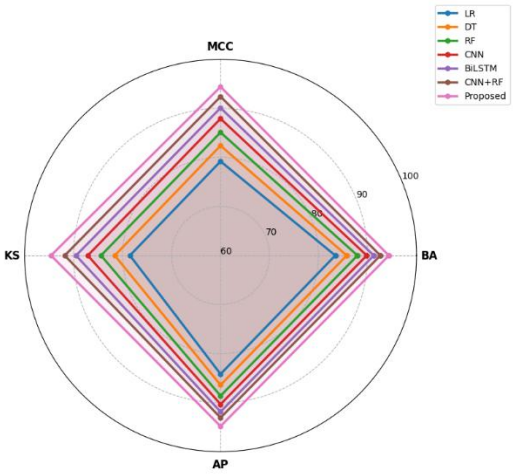

Fig 5. Radar chart showing the detection of frauds for the Bar code.

Figure 5 shows the fraud detection using the radar chart by which the figure will explain the whole model.

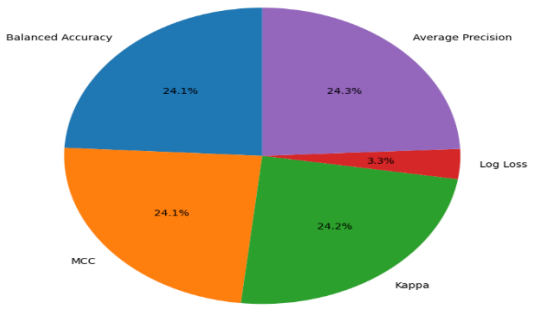

Fig 6 Pie chart displaying the results

The Pie chart in the Figure 5 shows the increase in the model's efficiency by grouping the other models and the new proposed model.

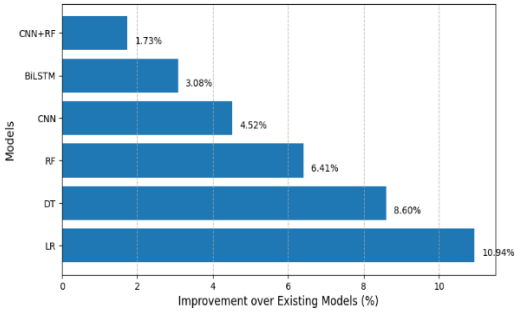

Fig. 7 Proposed Models Performance

The Figure 7 shows the performance of the proposed model where the lowest value gives the best approach.

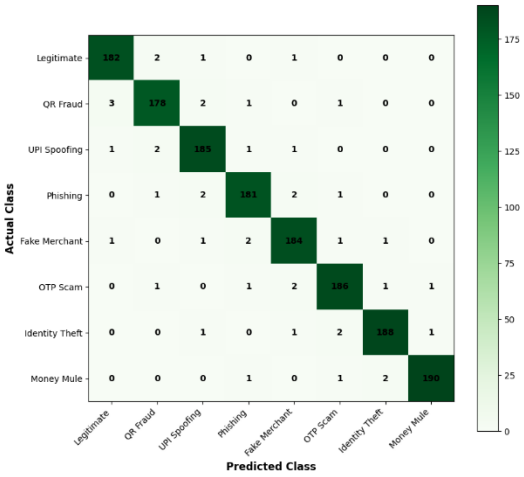

Fig. 8 Confusion Matrix

The Figure 8 shows the confusion matrix of the whole system by implementing the new environment.

CONCLUSION

The advent of digital payment platforms especially the Unified Payments Interface (UPI) and QR code-based payment systems have transformed the financial space by offering a secure, real-time and cashless mode of transaction. This broad acceptance has also opened up new avenues for cybercriminals to take advantage of vulnerabilities via phishing attacks, fake QR codes, identity theft, social engineering, unauthorised account access and fraudulent transaction activities. Traditional fraud detection methods largely rely on static validation methods and fixed rules. The techniques are not sufficient to detect complex, dynamic fraud schemes in real-time environments. These limitations highlight the critical need

for a smart, adaptable and highly accurate fraud detection model that can give improved transaction security and seamless user experience. To address these issues, this research proposed a Hybrid Machine Learning Model for UPI QR Code Fraud Detection and Secure Online Payment Authentication. The proposed model combines advantages of Convolutional Neural Network (CNN), Bidirectional Long Short-Term Memory (BiLSTM) and Extreme Gradient Boosting (XGBoost). The CNN part is efficient in extracting high level transaction features from large scale payment data and the BiLSTM model can learn sequential dependencies and behavioural transaction patterns which are difficult to find with traditional machine learning algorithms. Finally, XGBoost integrates the extracted deep features and reduces the misclassification rate by gradient boosting to achieve robust classification. This hybrid architecture combines deep learning and ensemble learning to improve the ability of fraud detection, generalisation and reduce false alarm rates compared with individual machine learning algorithms.

Prior to the training of the model, a data preparation pipeline is implemented for data quality enhancement and model learning efficiency. Missing values were imputed, duplicate records were deleted, categorical variables were encoded and numerical features were scaled to have the same distribution of features. Feature engineering and feature selection methods were used to identify the most relevant transaction features including transaction amount, payment frequency, device information, merchant details, user behaviour, timing of transaction and geographical location to further optimise the model's discriminative ability. The proposed model could better differentiate between legitimate transactions and fraudulent activities by employing these carefully selected features, as well as minimising unnecessary computational complexity.

The proposed framework was validated by comparison with different machine learning and normal algorithms for deep learning such as Logistic Regression, Decision Tree, Random Forest, CNN, BiLSTM and CNN with Random Forest. The performance was evaluated using several metrics specifically designed for highly imbalanced fraud detection datasets. These metrics include Balanced Accuracy, Matthews Correlation Coefficient (MCC), Cohen's Kappa Score, Log Loss and Average Precision (AP). The experimental results also demonstrated that the proposed hybrid model can outperform all the baseline models on all the evaluation metrics. The model has shown better performance in terms of balanced classification, predicted class vs actual class agreement, prediction error and precision-recall characteristics which indicates that it can accurately detect fraudulent UPI transactions with least false positives and false negatives.

The work also adds value by applying a secure multi-factor authentication (MFA) framework after estimation of the probability of fraud. The proposed system does not only depend on transaction classification but also consist of adaptive authentication mechanisms like OTP verification, Biometric authentication , PIN validation and trusted device verification during high risk transaction detection. The layered security architecture significantly strengthens payment authentication by preventing unauthorised transactions, even if suspicious payment attempts manage to bypass the first fraud detection. Therefore, the proposed framework offers proactive fraud prevention and reactive authentication which boosts the security for end users, financial institutions, merchants and payment service providers.

The presented model utilises an adaptive learning mechanism to update the fraud detection database with the newly validated transaction patterns. This allows the system to learn from new fraud types and evolving cyber risks without having to be completely rebuilt. Such adaptability is particularly valuable in today's digital payment ecosystems, where fraud techniques change rapidly and static detection systems become obsolete in a short time. Continuous learning increases the long-term robustness and guarantees a stable detection performance in real-world deployment settings.

To summarise, this work demonstrates that deep learning feature extraction, sequential behavioural analysis, ensemble classification and adaptive authentication can be combined to provide a holistic solution to secure UPI QR code payment systems. The proposed hybrid framework improves the accuracy of fraud detection, reduces financial losses, enhances customer trust and helps in building a safer and more reliable digital payment ecosystem. As digital financial transactions become more popular worldwide, intelligent fraud detection systems like the one proposed in this paper will be necessary to protect users from more sophisticated cyber-attacks.

Future work can extend this by using transformer-based architectures, graph neural networks for fraud network analysis, explainable artificial intelligence (XAI) to improve model transparency, blockchain-enabled transaction verification, federated learning for privacy-preserving distributed training, and real-time streaming analytics for immediate fraud response. These improvements can help make intelligent fraud detection systems more effective in protecting next generation digital

payment infrastructure by improving scalability, interpretability and resilience.

Acknowledgement

The author would like to appreciate the effort of the editors and reviewers.

Author Contributions

All authors are equally contributed.

Conflict of Interests

The authors declare that they have no conflicts of interest.

Ethics Approval

There are no human subjects in this article and informed consent is not applicable.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not- for-profit sectors.

REFERENCES

1. Gochhwal R. Unified Payment Interface—An Advancement in Payment Systems. American Journal of Industrial and Business Management. 2017;07(10):1174–91. doi:10.4236/ajibm.2017.710084
2. Neema K, Neema A. UPI (Unified Payment Interface)-A new technique of Digital Payment: An Explorative study. International Journal of Current Research in Multidisciplinary (IJCRM) [Internet]. 3(10):1–10. Available from: https://www.india-briefing.com/news/growth-of-digital-payments-systems-in-india-
3. Khan Z. AN IN-DEPTH ANALYSIS OF THE UPI PAYMENT SYSTEM IN INDIA. Vol. 55. 2023.
4. Sunil SV, Nalwaya DrN. Digital Payment Systems – An Overview of Categories and Extant Opportunities and Challenges. Int J Res Appl Sci Eng Technol. 2023 Apr 30;11(4):211–7. doi:10.22214/ijraset.2023.50019
5. A STUDY ON THE ADOPTION AND USER EXPERIENCE OF DIGITAL PAYMENT SYSTEMS AND UPI AMONG DIFFERENT AGE DEMOGRAPHICS.
6. Singh S, Jatana N, Sehgal S, Anand R, Arunkumar B, Ramesh JVN. Making Digital Payments Accessible Beyond Sight: A Usability Study of UPI-Based Smartphone Applications. IEEE Access. 2024;12:6830–41. doi:10.1109/ACCESS.2023.3348840
7. Kumar A, Vyas T, Ahmed S, Girdharwal N, Vijayakumar E, Thangavelu A. Security and Privacy Enabled Framework for Online Social Networks using Blockchain. In: 2023 4th International Conference on Electronics and Sustainable Communication Systems, ICESC 2023 - Proceedings. Institute of Electrical and Electronics Engineers Inc.; 2023. p. 641–7. doi:10.1109/ICESC57686.2023.10193119
8. Bhattacharya S, Singla B. The Role of QR Code Technology in Revolutionizing Banking. Journal of Computers, Mechanical and Management. 2024 Aug 4;3(3):36–45. doi:10.57159/gadl.jcmm.3.3.240121
9. Bradford T, Hayashi F, Toh YL. Developments of QR Code-Based Mobile Payments in East Asia. 2019.
10. Nugroho MA, Hariyanto D, Nugraha RAZ, Dawood AK. QR Code Payment Acceptance and Its Impact on SMEs Sustainability Performance. Journal of Research, Innovation and Technologies. 2026 Jan 7;5(1):1–21. doi:10.56578/jorit050101
11. Bharadwaj M, Rajarajeshwari BN. Digital Forensics Challenges in UPI Fraud, QR Scam and Online Payment Theft— A Review. In. 2026. p. 287–95. Available from: https://www.atlantis-press.com/doi/10.2991/978-94-6239-610-4_27 doi:10.2991/978-94-6239-610-4_27
12. Dattathrani S, Dé R. | P a g e Security in Mobile Payments: A Report on User Issues. 2017.
13. Gochhwal R. Unified Payment Interface—An Advancement in Payment Systems. American Journal of Industrial and Business Management. 2017;07(10):1174–91. doi:10.4236/ajibm.2017.710084
14. Bharadwaj M, Rajarajeshwari BN. Digital Forensics Challenges in UPI Fraud, QR Scam and Online Payment Theft— A Review. In. 2026. p. 287–95. doi:10.2991/978-94-6239-610-4_27
15. Invalli S. Digital Payment Patterns in India: A Cross-Sectional Study of Credit Cards, Debit Cards, and Unified Payments Interface (UPI) Trends. Cureus Journal of Business and Economics. 2025 Jul 3. doi:10.7759/s44404-025-04075-7
16. Kolte DM, Humbe VR. Study of UPI/BHIM Payment System in India. International Journal of Science and Research. doi:10.21275/SR201202182305
17. Ali A, Abd Razak S, Othman SH, Eisa TAE, Al-Dhaqm A, Nasser M, et al. Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review. Applied Sciences (Switzerland). MDPI; 2022. doi:10.3390/app12199637
18. Prasad G, Kumar H, Nagesh V, Manikanth B, Kiran S. Enhancing Performance of Financial Fraud Detection Through Machine Learning Model. J Contemp Edu Theo Artific Intel. 2023;101. doi:10.47991/2996-4954/JCETAI-101

19. Islam S, Haque MM, Karim ANMR. A rule-based machine learning model for financial fraud detection. International Journal of Electrical and Computer Engineering. 2024 Feb 1;14(1):759–71. doi:10.11591/ijece.v14i1.pp759-771
20. Khalid AR, Owoh N, Uthmani O, Ashawa M, Osamor J, Adejoh J. Enhancing Credit Card Fraud Detection: An Ensemble Machine Learning Approach. Big Data and Cognitive Computing. 2024 Jan 1;8(1). doi:10.3390/bdcc8010006
21. Jagadeesan S, Arjun KS, Dhanika G, Karthikeyan G, Deepika K. UPI fraud detection using machine learning. In: Challenges in Information, Communication and Computing Technology [Internet]. London: CRC Press; 2024. p. 755–60. Available from: https://www.taylorfrancis.com/books/9781003559085/chapters/10.1201/9781003559085-130 doi:10.1201/9781003559085-130
22. Lakshmi LD, B. Sravanthi, Raju ASP, Sadvika BG, Nayak BV. HYBRID DEEP LEARNING MODEL FOR UPI FRAUD DETECTION USING CNN AND RANDOM FOREST. Journal of Nonlinear Analysis and Optimization. 2025;16(01):201–7. doi:10.36893/jnao.2025.v16.i01.026
23. Vinayak Mahale S, Sopan More S, Akhtar Shaikh A, Jaykumar Patil B. Studies and Development AI-POWERED UPI FRAUD DETECTION AND ALERT SYSTEM. www.ijamrsd.com | Journal of Advanced Multidisciplinary Research [Internet]. Available from: www.ijamrsd.com
24. Gupta S. Securing Unified Payments Interface: A Deep Learning Approach for Fraudulent Transaction Detection. Journal of Global Research in Multidisciplinary Studies [Internet]. JGRMS; 2025. Available from: https://saanvipublications.com/journals/index.php/jgrms/index
25. Ganmati A, Afdel K, Koutti L. Deep Learning-Based Multi-Factor Authentication: A Survey of Biometric and Smart Card Integration Approaches [Internet]. 2025 Oct 4. Available from: http://arxiv.org/abs/2510.05163
26. Markkandeyan S, Ananth AD, Rajakumaran M, Gokila RG, Venkatesan R, Lakshmi B. Novel hybrid deep learning based cyber security threat detection model with optimization algorithm. Cyber Security and Applications. 2025 Dec 1;3. doi:10.1016/j.csa.2024.100075
27. Zahid M, Bharati TS. Enhancing cybersecurity in IoT systems: a hybrid deep learning approach for real-time attack detection. Discover Internet of Things. 2025 Dec 1;5(1). doi:10.1007/s43926-025-00156-y
28. Abbas A, Salahuddin M, Khan MZ, Khan AA, Zaman FU, Inam SA, et al. Machine learning-based hybrid technique to enhance cyber-attack perspective. Journal of Cloud Computing. 2025 Dec 1;14(1). doi:10.1186/s13677-025-00782-5
29. Bouzaachane K, Guarmah EM El, Alnajim AM, Khan S. Addressing Modern Cybersecurity Challenges: A Hybrid Machine Learning and Deep Learning Approach for Network Intrusion Detection. Computers, Materials and Continua. 2025;84(2):2391–410. doi:10.32604/cmc.2025.065031
30. Muhammad Salman Bukhari S, Zafar MH, Houran MA, Qadir Z, Kumayl Raza Moosavi S, Sanfilippo F. Enhancing cybersecurity in Edge IIoT networks: An asynchronous federated learning approach with a deep hybrid detection model. Internet of Things (Netherlands). 2024 Oct 1;27. doi:10.1016/j.iot.2024.101252
31. Online Payment Fraud Detection [Internet]. [cited 2026 Jul 14]. Available from: https://www.kaggle.com/datasets/jainilcoder/online-payment-fraud-detection/data?