Detecting and Preventing Fraud in QR Code-Based Mobile Payment Systems

Team Q.E.D

1 Introduction

The rapid adoption of mobile payment systems leveraging QR codes has revolutionized transactions, making them faster and more accessible. However, this convenience comes with significant security risks, such as static QR code fraud, expired dynamic codes, and identity theft. Ensuring the safety of these systems is critical to maintaining user trust and preventing financial loss. This project aims to develop an AI-driven solution to detect and mitigate fraud in QR code-based payment systems, addressing these challenges with innovative and scalable approaches.

2 Methodology

2.1 Modeling Approach

The payment system flow was modeled by identifying the key actors and their interactions:

- **QR Code:** Encodes transaction details such as merchant information and payment amount.
- **Customer:** Initiates payments using mobile devices.
- **Merchant:** Generates and shares QR codes for receiving payments.
- **Transaction:** Digital representation of the payment between the customer and merchant.
- **API Gateway:** Processes and validates transaction data.
- **Fraud Detection System:** Analyzes transaction data to identify potential fraud.

This flow highlights potential vulnerabilities where attackers could intercept QR codes, manipulate transaction data, or exploit backend systems.

2.2 Exploration of Existing Solutions

To guide our framework design, we studied existing datasets and solutions:

- **IEEE-CIS Fraud Detection Dataset:** Provided insights into real-world fraud patterns.
- **PaySim Synthetic Financial Datasets:** Simulated realistic scenarios of mobile payment fraud.

These resources informed our understanding of fraud mechanisms and inspired the development of an effective and scalable solution.

3 Conceptual Framework

The conceptual framework for detecting and preventing fraud in QR code-based mobile payment systems is structured around three primary components: Solution, Datasets, and Technical Infrastructure.

3.1 Solution

Our solution leverages advanced AI models to learn and identify fraudulent patterns within QR code-based payment systems. The approach is divided into two main areas:

3.1.1 QR Code Validation

QR code validation serves as the first line of defense against fraud. This process ensures that the QR codes used in transactions are authentic and have not been tampered with.

By implementing robust QR code validation, the system can effectively block malicious QR codes from initiating fraudulent transactions.

3.1.2 Behavior Analysis for Fraud Detection

Beyond QR code validation, analyzing user and merchant behaviors provides deeper insights into potential fraud. This involves:

- **Transaction Pattern Analysis**: Monitoring transaction amounts, frequencies, and timestamps to identify anomalies that deviate from typical behavior.
- **Geolocation Tracking**: Comparing the geolocation of the customer with historical data to detect unusual transaction locations.
- **Device Fingerprint Analysis**: Ensuring that the device used for the transaction matches the known device fingerprint of the customer to prevent identity theft.
- **Merchant Activity Monitoring**: Assessing the transaction volumes and QR code generation logs of merchants to detect irregularities that may indicate fraudulent activities.

By integrating behavioral analysis, the AI models can detect sophisticated fraud attempts that may bypass basic QR code validations.

3.2 Datasets

The effectiveness of AI models in detecting fraud heavily relies on the quality and relevance of the datasets used for training and evaluation. Given the sensitive nature of transaction data, public datasets specific to QR code-based payment systems are scarce. To address this gap, we adopted a synthetic data generation approach tailored to mimic real-world scenarios.

3.2.1 Challenges in Obtaining Data

According to [1], the paucity of public datasets in fraud detection research is primarily due to the sensitivity and confidentiality of transaction data. This limitation necessitates innovative approaches to data generation that preserve the statistical properties of real transactions while ensuring privacy.

3.2.2 Synthetic Data Generation

To simulate a realistic dataset for QR code-based transactions, we developed a comprehensive synthetic data generation process. This approach ensures that the generated data closely mirrors real-world transaction patterns while incorporating various fraud scenarios. The synthetic data generation process encompasses several key stages:

Customer and Merchant Profiles Profiles for customers and merchants were generated with geolocations clustered around major Algerian cities, specifically Algiers, Oran, and Constantine. Each customer profile includes a unique identifier, geographic coordinates, and a device fingerprint to facilitate behavior analysis. Similarly, merchant profiles contain unique identifiers, geolocations, and metrics such as transaction volume and QR code generation logs.

Transaction Simulation A substantial number of transactions were simulated to ensure a robust dataset. Each transaction record comprises attributes such as transaction ID, amount, timestamp, status, QR code type (static or dynamic), encoded data integrity, reuse flags, and geolocation coordinates of both the customer and the merchant. Dynamic QR codes were assigned expiration times to reflect their limited validity period.

Fraud Injection To imbue the dataset with realistic fraud cases, specific fraud scenarios were systematically introduced based on predefined patterns. These fraud cases include:

- **Tampered Static QR Code**: Altering the encoded data to redirect funds.
- **Fake Static QR Code**: Assigning unrelated or fake URLs.
- **Identity Theft via Device Fingerprint**: Using device fingerprints from other customers.
- **Geolocation Anomalies**: Assigning geolocations inconsistent with the customer's usual locations.
- **Malformed Encoded Data**: Inserting invalid formats into the QR code data.
- **Large Transaction Amounts**: Generating transactions with unusually high amounts.
- **Frequent Transactions**: Simulating multiple transactions within short timeframes.
- **Invalid Checksum QR Codes**: Creating QR codes with invalid checksums.
- **Repeated QR Code Usage**: Monitoring and flagging excessive reuse of QR codes.

Each fraudulent transaction was carefully designed to reflect realistic attack vectors, enhancing the dataset's utility for training AI models to recognize diverse fraud patterns.

3.2.3 Synthetic Dataset Characteristics

The generated dataset encompasses the following characteristics:

- **Volume**: 100,000 transactions ensure a sufficient volume for training robust AI models.
- **Features**: Includes attributes such as transaction amount, timestamp, status, QR code type, encoded data integrity, reuse flags, and geolocation coordinates.
- **Fraud Representation**: 5% of the transactions are labeled as fraudulent, encompassing various fraud cases to provide a diverse training ground for the AI models.
- **Geospatial Clustering**: Transactions are geographically clustered around major cities to reflect realistic user and merchant distributions.
- **Behavioral Attributes**: Incorporates device fingerprints and merchant activity logs to facilitate in-depth behavioral analysis.

3.3 AI Models Training and Evaluation

Models were trained using a stratified split to maintain the fraud-to-normal transaction ratio. Evaluation metrics included precision, recall, F1-score, and the Area Under the Receiver Operating Characteristic Curve (AUC-ROC) to assess model performance comprehensively.

Our models focus primarily on QR code validation and behavior analysis for fraud detection.

3.3.1 QR Code Validation Models

QR Code Validation Models are essential for ensuring the authenticity and integrity of QR codes used in transactions.

Computer Vision Model The model classifies QR codes as benign or malicious using a CNN with convolutional, pooling, and dense layers, trained with binary cross-entropy loss on grayscale images.The model achieving 99.95 validation accuracy after one epoch

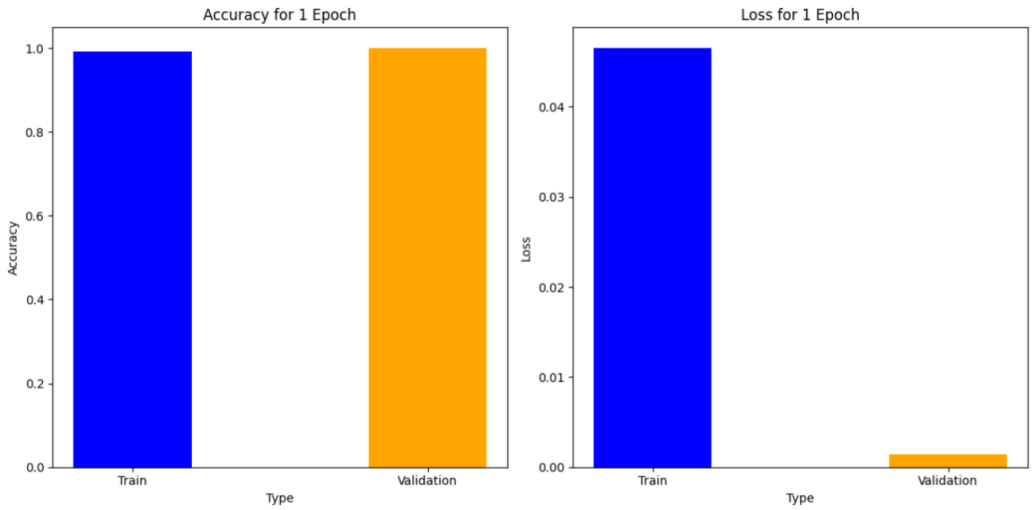

Figure 1: Accuracy and loss Metrics for Computer Vision Model

Natural Language Processing (NLP) Model The NLP model (LSTM) is designed to validate QR code data by analyzing URLs and their accompanying descriptions to identify and classify fraudulent patterns.

Validation Metrics: Accuracy

3.3.2 Behavior Analysis for Fraud Detection

Behavior Analysis Models play a crucial role in identifying fraudulent activities by examining patterns and anomalies in user and merchant behaviors.

Ensemble Model (XGBoost) The model is trained on our synthetic data to predict wether a given transaction is fraudulent or not , it analysed and used in its training data behaviours of both the merchant and the customer.

Validation Metrics: XGBoost achieved an AUC metric of 0.92

3.3.3 Prevention model

Prevention Models leverage reinforcement learning to create adaptive agents that can proactively prevent fraudulent transactions in real-time. These models continuously learn and improve their decision-making strategies by interacting with the transaction environment, enabling them to dynamically adjust to emerging fraud patterns and enhance the overall security of the mobile payment system.

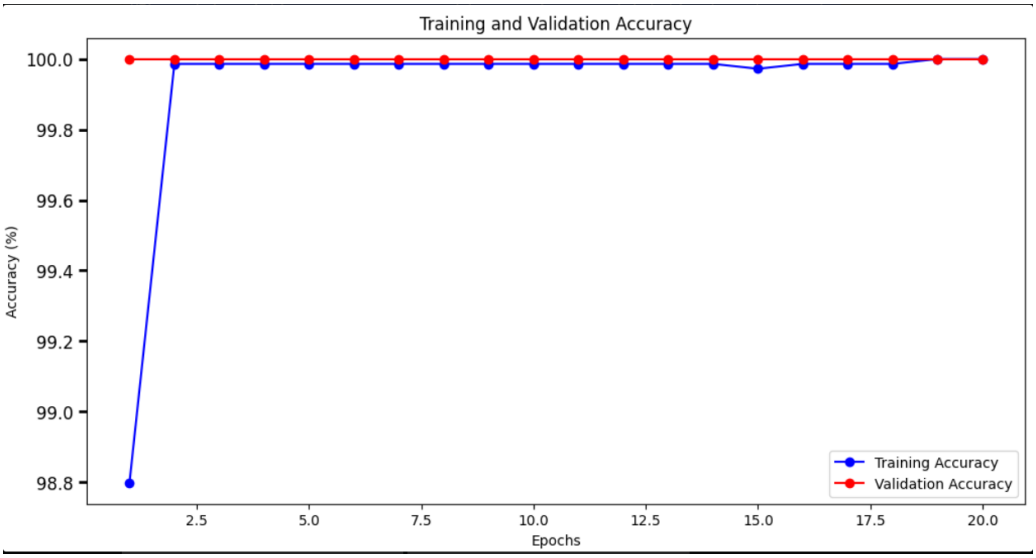

Figure 2: Validation Metrics for the NLP Model

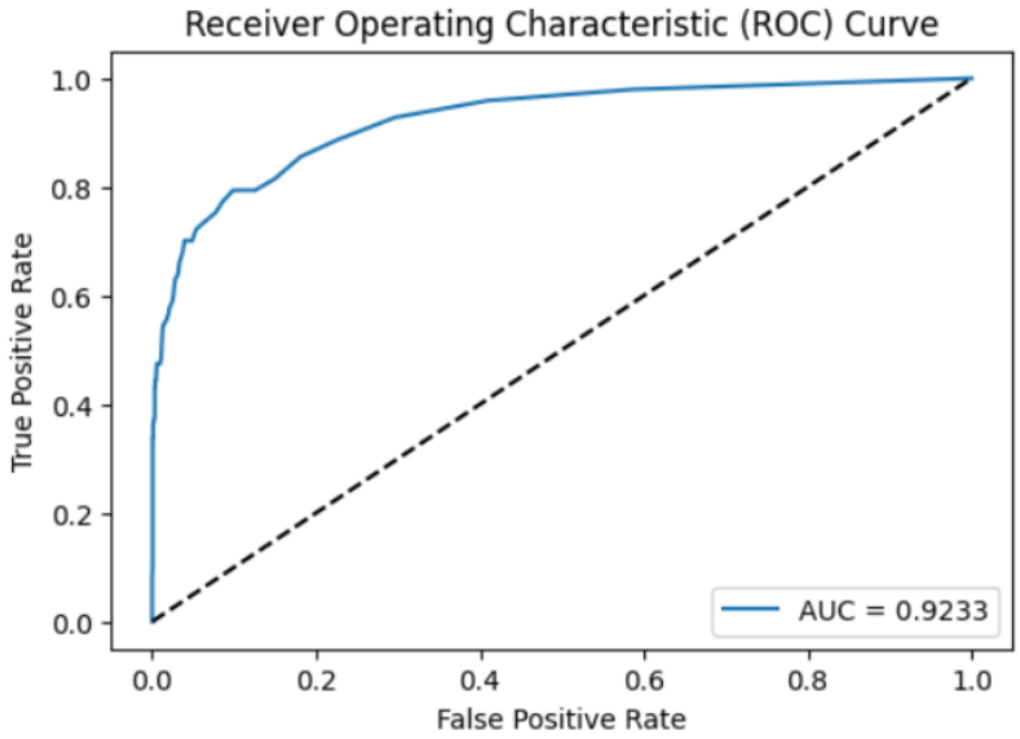

Figure 3: AUC graph for XGBoost model

Prevention Smart Agent using Reinforcement Learning Task: The reinforcement learning agent actively monitors each transaction in real-time, making decisions to approve or reject based on learned policies to effectively prevent fraudulent activities. The agent was trained using Deep-Q Learning algorithm .

Training Data: The agent was trained using simulated transaction streams generated by the QR Code Fraude Detection environment, encompassing both legitimate and fraudulent transactions to enable the agent to learn optimal decision-making strategies through iterative interactions.

3.4 Scalability

Ensuring scalability is vital for deploying the fraud detection system in real-world, high-volume environments. Our approach addresses scalability through:

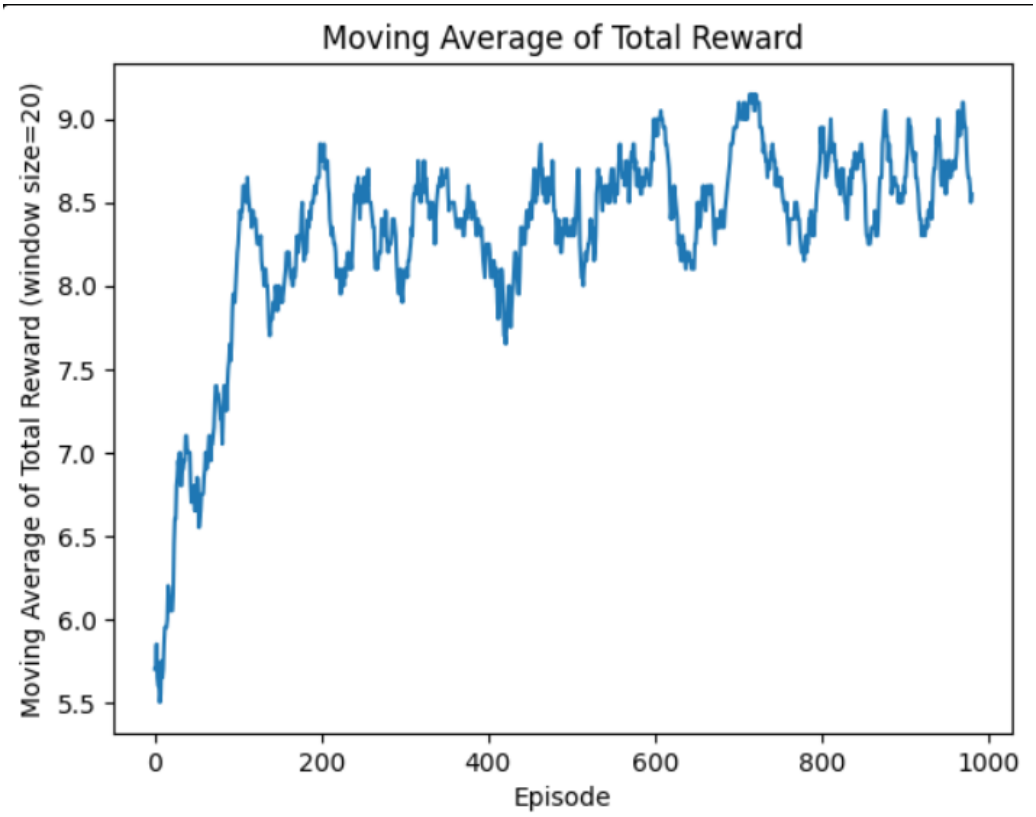

Figure 4: Performance Plots for Prevention Smart Agent using Reinforcement Learning

- **Model Optimization**: Implementing techniques such as model pruning and quantization to reduce computational overhead.
- **Containerization**: Dockerizing models to ensure seamless deployment, scalability, and portability across different environments.
- **Federated Learning**: For real data training, given the sensitivity of transaction data, we plan to replace our pipeline of training models with real data by leveraging federated learning, ensuring privacy and security while enabling scalable model updates.

4 Discussion

4.1 Innovation

Our approach introduces several unique elements that distinguish it from existing fraud detection solutions in QR code-based mobile payment systems. Firstly, the integration of both QR code validation and comprehensive behavior analysis provides a multi-layered defense mechanism. While many existing systems focus solely on transaction monitoring, our solution ensures the authenticity of QR codes themselves, effectively preventing fraud at the foundational level. Additionally, the use of advanced AI models, including computer vision for QR code integrity and natural language processing for data validation, enables the detection of sophisticated fraudulent patterns that traditional methods might overlook.

Another innovative aspect is our synthetic data generation methodology. Given the scarcity of public datasets specific to QR code transactions, our approach to creating realistic and diverse synthetic datasets ensures that the AI models are trained on data that closely mirrors real-world scenarios. This not only enhances the robustness of the models but also maintains data privacy and security. Furthermore, the incorporation of reinforcement learning

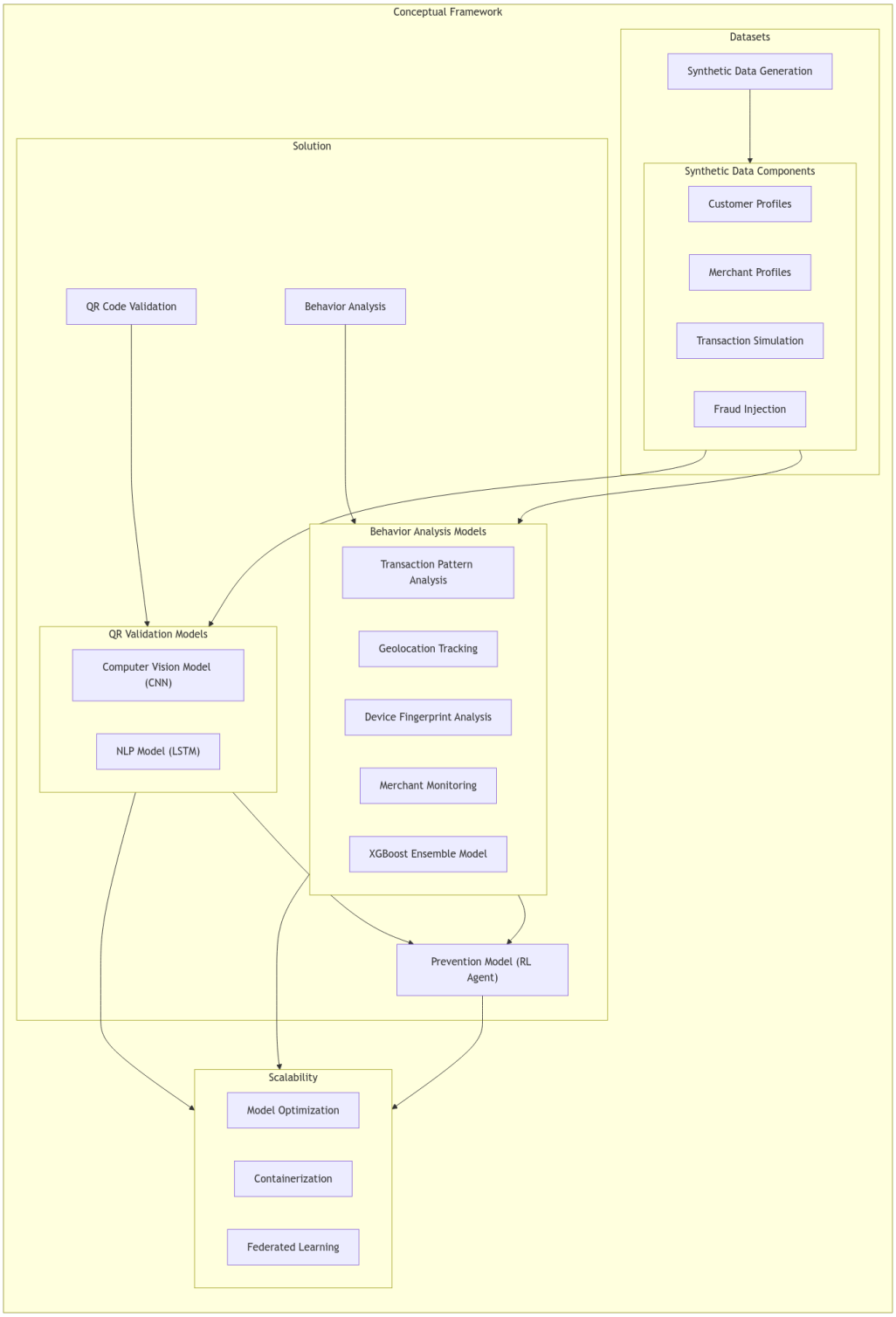

Figure 5: General overview of the solution framework

for the prevention smart agent represents a forward-thinking strategy, allowing the system to adapt dynamically to emerging fraud tactics in real-time.

4.2 Challenges Faced

Developing a robust fraud detection system for QR code-based payments presented several technical and resource-related challenges. One of the primary obstacles was the lack of publicly available datasets tailored to QR code transactions. To overcome this, we implemented a synthetic data generation process that accurately simulates

real-world transaction behaviors and fraud scenarios. Ensuring the realism and variability of the synthetic data required careful calibration and validation to maintain the statistical properties of actual transactions.

Another significant challenge was the computational complexity associated with training multiple AI models, including computer vision, NLP, and ensemble algorithms. Optimizing these models to achieve high performance without compromising scalability necessitated the application of model pruning and quantization techniques. Additionally, integrating reinforcement learning for proactive fraud prevention introduced complexities in designing an effective learning environment and ensuring the agent's decision-making processes were both accurate and efficient.

Resource constraints, such as limited access to high-performance computing infrastructure, also posed challenges. We addressed these by leveraging containerization with Docker to streamline deployment and facilitate scalability across different environments. Ensuring data privacy and security during model training, especially when considering federated learning for real data incorporation, required meticulous implementation of secure protocols and adherence to best practices in data handling.

4.3 Future Improvements

While the current framework demonstrates significant efficacy in fraud detection and prevention, several areas offer opportunities for enhancement. One potential improvement is the incorporation of real transaction data through federated learning. This approach would allow our models to benefit from real-world data while maintaining privacy and security, thereby improving their accuracy and adaptability to evolving fraud patterns.

Expanding the behavioral analysis to include additional contextual factors, such as temporal trends and socio-economic indicators, could further refine the model's predictive capabilities. Integrating more advanced AI techniques, such as deep learning architectures and unsupervised anomaly detection methods, may enhance the system's ability to identify previously unknown fraud strategies.

Another area for future development is the enhancement of the prevention smart agent using more sophisticated reinforcement learning algorithms. This could involve multi-agent systems that collaborate to detect and mitigate complex fraud scenarios or the implementation of transfer learning to adapt policies across different regions and transaction types.

Furthermore, improving the scalability and real-time processing capabilities of the system will be crucial as the volume of QR code transactions continues to grow. Investing in distributed computing resources and optimizing the infrastructure for low-latency processing will ensure that the system remains effective in high-demand environments.

Lastly, conducting extensive field trials and gathering feedback from real-world deployments will provide invaluable insights into the system's performance and areas for improvement. This iterative approach will facilitate the continuous evolution of the fraud detection framework, ensuring its relevance and effectiveness in combating fraud in the dynamic landscape of mobile payments.

5 Conclusion

In our solution, we have developed a robust framework for detecting and preventing fraud in QR code-based mobile payment systems. By integrating advanced QR code validation techniques with comprehensive behavior analysis, our approach effectively identifies and mitigates various fraudulent activities. The utilization of synthetic data generation allowed us to train reliable AI models despite the lack of publicly available datasets, ensuring both practicality and scalability.

Our implementation of computer vision and natural language processing models for QR code integrity, combined with ensemble and reinforcement learning models for behavior analysis and prevention, demonstrates the efficacy of a multi-layered defense strategy. Additionally, the focus on scalability through model optimization, containerization, and federated learning prepares our framework for deployment in real-world, high-volume environments.

Future work will focus on incorporating real transaction data to further enhance model accuracy, expanding the scope of behavioral analysis, and conducting extensive field trials to validate system performance. Overall, this framework provides a solid foundation for enhancing the security and reliability of QR code-based mobile payment systems, contributing to safer and more trustworthy digital transaction ecosystems.

References

[1] *Applying Simulation to the Problem of Detecting Financial Fraud*, Faculty of Computing, Department of Computer Science and Engineering, `https://bth.diva-portal.org/smash/record.jsf?pid=diva2:955852&dswid=-5394`.