SafeScan : Proactive Fraud Detection in Digital Payments using ML

B. SUDHA MADHURI
Assistant Professor
Information Technology
Vignan's Institute of Engineering for Women
Visakhapatnam, India
sudhamadhuri10863@gmail.com

JILLIDIMUDI LALITHA VASAVI
Information Technology
Vignan's Institute of Engineering for Women
Visakhapatnam, India
lalithavasavi12@gmail.com

MUNAKALA PRIYA
Information Technology
Vignan's Institute of Engineering for Women
Visakhapatnam, India
munakalapriya1234@gmail.com

KRISHNA VINEETHA PATNAIK KUPPILI
Information Technology
Vignan's Institute of Engineering for Women
Visakhapatnam, India
vineethapat15@gmail.com

PANDURI RAKSHITHA RATNA SAI
Information Technology
Vignan's Institute of Engineering for Women
Visakhapatnam, India
rakshithatp239@gmail.com

***Abstract*—Fraud in digital payments poses a significant threat to user security, requiring robust measures for prevention and detection. The proposed project, SafeScan, offers a comprehensive solution to address these challenges by developing an integrated system for proactive fraud detection in digital payments. The system employs advanced validation mechanisms to verify QR codes and UPI IDs, ensuring the authenticity of payment details while detecting tampering or spoofing. Concurrently, Machine Learning algorithms are utilized to analyze transaction patterns, including frequency, amount, and user behavior, to identify anomalies indicative of fraudulent activity. SafeScan also features an automated response system that blocks transactions flagged as suspicious and notifies users in real-time, empowering them to take immediate action. Additionally, the system provides an admin dashboard for real-time monitoring ensuring adaptability to emerging fraud tactics. By transmitting transactional and fraud detection data to a centralized platform for visualization and analysis, users can remotely monitor activity and make informed decisions. SafeScan aims to revolutionize digital payment security by offering an intelligent, scalable, and user-friendly solution, thereby fostering trust and confidence in the financial ecosystem.**

Keywords— Python, Machine Learning, Flask Integration, Scikit, Database, QR Scanner, Transaction Patterns, Fraud Detection.

I. INTRODUCTION

Digital payments have revolutionized the way individuals and businesses handle financial transactions, offering unparalleled convenience, speed, and accessibility. The rise of platforms enabling cashless transactions has accelerated economic activities and facilitated seamless exchanges of goods and services. However, the widespread adoption of these systems has also introduced new vulnerabilities, making them prime targets for fraudsters. Activities such as spoofed UPI IDs, tampered QR codes, phishing attempts, and other sophisticated techniques pose significant threats to users and financial institutions alike. To address these challenges, the proposed project, SafeScan, seeks to deliver an innovative, machine learning-driven solution for real-time fraud detection in digital payments. The increasing dependency on digital payment systems has led to a surge in fraudulent activities, causing significant financial losses to individuals and businesses. Existing fraud detection systems often fail to operate in real-time and struggle to adapt to evolving attack strategies. The motivation behind SafeScan stems from the need to provide a secure, intelligent, and proactive fraud detection mechanism that not only identifies fraudulent transactions but also prevents them before they occur. By leveraging the power of machine learning, this project aims to create an adaptive system that continuously learns from transaction patterns, ensuring enhanced security for users. SafeScan also addresses the lack of awareness among users by providing real-time alerts and actionable insights. Ultimately, the project aspires to strengthen trust in digital payment ecosystems by making transactions safer and more reliable, fostering widespread adoption and financial security. With the rapid growth of digital payments, financial fraud has become a pressing concern, resulting in significant monetary losses and a decline in user trust. Fraudsters exploit vulnerabilities in payment systems by tampering with QR codes, spoofing UPI IDs, and using sophisticated phishing techniques. Existing fraud detection mechanisms primarily rely on predefined rule-based approaches, which struggle to keep up with evolving fraud patterns and often fail to provide real-time security. The SafeScan project aims to address these challenges by developing an intelligent fraud detection system that leverages machine learning algorithms for proactive fraud prevention. The system will analyze transaction patterns, validate QR codes and UPI IDs, and alert users in real-time if fraudulent activities are detected. By ensuring secure and transparent digital transactions, SafeScan aims to minimize fraud, protect users, and enhance the reliability of digital payment platforms. The primary goal of SafeScan is to create a proactive fraud detection system that ensures secure digital transactions by leveraging advanced technologies such as Machine Learning (ML) and real-time validation. This project aims to verify payment Integrity like ensuring the authenticity of QR codes and UPI IDs to prevent tampering and spoofing, identify fraud patterns like analyzing transaction behaviors using ML algorithms to detect anomalies and flag suspicious activities and enhance user trust like fostering confidence in digital payment systems by providing a secure, user-friendly, and reliable solution. Despite significant advancements in digital payment infrastructure, fraud remains a critical issue. Common challenges include QR Code Tampering, where fraudsters manipulate QR codes by embedding malicious links or altering payment details, leading unsuspecting users

to make payments to fraudulent accounts. Another challenge is Spoofed UPI IDs, where fraudulent actors create UPI IDs that mimic legitimate accounts to deceive users into transferring funds to unauthorized entities. Additionally, traditional fraud detection systems often fail to operate in real-time, allowing fraudulent transactions to be completed before any preventive measures are taken. Cybercriminals continuously develop new methods to exploit vulnerabilities in digital payment systems, making static security mechanisms inadequate. Furthermore, many users lack the knowledge to identify fraudulent activities, making them more susceptible to scams. SafeScan aims to tackle these issues by providing a dynamic and intelligent fraud detection system that ensures secure and reliable digital transactions.

II. Related Work

[1] The study presents a machine learning-based fraud detection system for digital payments, utilizing transaction pattern analysis and anomaly detection techniques. The model is evaluated using precision, recall, and F1-score metrics to ensure accuracy in identifying fraudulent transactions. [2] The paper examines real-time fraud prevention in UPI transactions using deep learning techniques. The system detects spoofed UPI IDs and phishing attempts by analyzing transaction metadata and behavioural patterns, reducing fraudulent activities. [3] A blockchain-based approach for securing digital payments is explored, integrating decentralized identity verification and transaction auditing. The proposed system enhances transparency and reduces fraud risks by eliminating single points of failure. [4] Traditional rule-based fraud detection mechanisms are being replaced by AI-driven solutions that adapt to evolving fraud tactics. These systems use ensemble learning and hybrid models to improve fraud detection accuracy and minimize false positives. [5] Machine learning-based fraud detection frameworks leverage supervised and unsupervised learning techniques to identify suspicious activities in digital payments. Researchers propose real-time anomaly detection algorithms that continuously learn from transaction data. [6] The paper introduces an AI-powered real-time fraud prevention system that integrates biometric authentication and behavioural analysis for securing online transactions. The proposed framework achieves over 95% accuracy in detecting fraudulent activities. [7] The study explores federated learning in fraud detection, where multiple financial institutions collaboratively train fraud detection models without sharing sensitive customer data. The system improves fraud detection rates while maintaining privacy. [8] An adaptive fraud detection approach is proposed, incorporating reinforcement learning to dynamically adjust fraud detection thresholds based on transaction risk levels. The system enhances fraud prevention while reducing unnecessary transaction blocks. [9] The paper presents a hybrid fraud detection model combining statistical analysis and deep learning. It identifies payment fraud by detecting deviations from normal transaction behaviour patterns. [10] A deep reinforcement learning-based fraud prevention system is introduced, which autonomously learns fraud patterns and refines detection strategies over time. The system effectively mitigates emerging fraud techniques in digital transactions. [11] The study discusses the importance of anomaly detection in digital payment security, proposing a hybrid model that integrates decision trees and neural networks for improved fraud detection. [12] The paper proposes an IoT-enabled secure payment system that uses AI-driven fraud detection combined with edge computing for real-time transaction analysis and fraud prevention. [13] Implementing real-time fraud detection using Graph Neural Networks (GNN) enhances security in digital payments by analyzing transaction networks and identifying fraudulent entities before transactions are processed. [14] The article presents a distributed fraud detection system using blockchain smart contracts, ensuring immutable transaction verification and reducing fraud in peer-to-peer digital payments. [15] An IoT-based fraud detection and prevention framework is introduced, leveraging AI and real-time monitoring for securing online transactions. The system enhances fraud detection efficiency in mobile and digital payment platforms.

III. Proposed Work

A. PROPOSED SYSTEM

SafeScan represents a significant advancement in fraud detection by leveraging the power of machine learning. Instead of relying on static rules, SafeScan employs sophisticated machine learning models that continuously learn and adapt from the vast amounts of transaction data they analyze. This dynamic learning process allows SafeScan to identify subtle patterns and anomalies that would be missed by traditional rule-based systems, significantly reducing the number of false positives. By minimizing these false alarms, SafeScan improves the overall efficiency of fraud detection, allowing analysts to focus on genuinely suspicious activity. Critically, SafeScan operates in real-time, providing immediate analysis of every transaction as it occurs. This real-time capability is crucial for proactive fraud prevention, enabling SafeScan to intervene and block potentially fraudulent transactions before they are completed, rather than simply flagging them after the fact. The core strength of SafeScan lies in its use of machine learning algorithms. These algorithms are designed to automatically adapt to new and evolving fraud tactics. As fraudsters develop new methods, SafeScan's models learn to recognize these changes, ensuring that the system remains effective even against previously unseen attack vectors. This continuous adaptation is a key differentiator from traditional systems that require manual updates to their rules. SafeScan's real-time transaction analysis provides granular insights into each transaction, assessing its risk level based on a multitude of factors. This allows for highly accurate fraud detection and prevention.

These real-time alerts empower users to take immediate action, such as verifying the legitimacy of the transaction or freezing their account, preventing any financial loss from occurring. This proactive approach not only protects users from financial harm but also fosters greater trust in the security of their financial transactions. SafeScan's strength lies in its strategic application of machine learning (ML) algorithms, which fundamentally enhance fraud detection across three key dimensions: accuracy, adaptability, and real-time monitoring. Traditional systems often struggle with accurately distinguishing between legitimate and fraudulent transactions, leading to high false positive rates. SafeScan's ML models, trained on vast datasets of transaction patterns, learn to identify subtle anomalies and suspicious behaviours that humans might miss, significantly improving the accuracy of fraud detection. Furthermore, the dynamic nature of fraud requires systems that can adapt to ever-evolving tactics. SafeScan's ML algorithms provide this crucial adaptability.

Beyond accuracy and adaptability, SafeScan's real-time monitoring capabilities are essential for proactive fraud prevention.

By analyzing transactions as they occur, SafeScan can identify and flag suspicious activity immediately, allowing for timely intervention and preventing fraudulent transactions from completing. This real-time approach is far more effective than traditional methods that often detect fraud only after the damage has been done. This multi-faceted approach, leveraging ML for enhanced accuracy, adaptability, and real-time monitoring, significantly mitigates the risks associated with digital payment fraud.

By proactively identifying and preventing fraudulent transactions, SafeScan fosters a safer and more secure transaction environment for both users and financial institutions. The comprehensive security mechanism offered by SafeScan goes beyond simply relying on ML-based fraud detection. The inclusion of QR code verification and UPI ID validation adds layers of security, ensuring that transactions are initiated and processed securely. This combination of advanced technologies creates a robust defence against fraud, surpassing the capabilities of traditional methods and making digital transactions safer, more reliable, and trustworthy for all stakeholders.

The block diagram illustrates the architecture of the SafeScan Web Application, designed to efficiently detect UPI fraud patterns and ensure secure transactions. The application follows a systematic approach to enable real-time fraud detection and prevention. Upon initialization, it loads essential components, including the database, frontend templates (HTML, CSS, JavaScript), and backend services. In addition to UPI verification, SafeScan incorporates various services, including QR code verification to detect tampered or malicious QR codes, database management for updating transaction records and fraud reports, and seamless communication between the model and backend servers to ensure smooth processing and fraud detection. By integrating these components, SafeScan provides a real-time, intelligent, and adaptive fraud detection mechanism, enhancing security and reliability in digital payments.

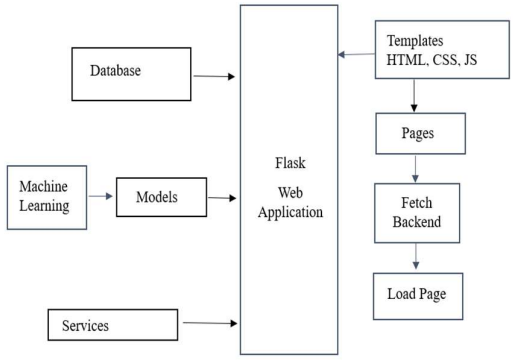

Fig. 1. Block Diagram.

When the SafeScan web application loads, it presents an input field for manual UPI ID entry and a QR scanner powered by the HTML5-QRCode.js library. This scanner extracts the UPI ID from the QR code, allowing users to either scan or manually enter the UPI ID. Upon submission, the application first checks the UPI ID against the database. If the ID is found and verified as safe, the system marks it as secure. However, if the UPI ID is not present in the database, it is sent to the fraud detection model for further analysis using machine learning algorithms.

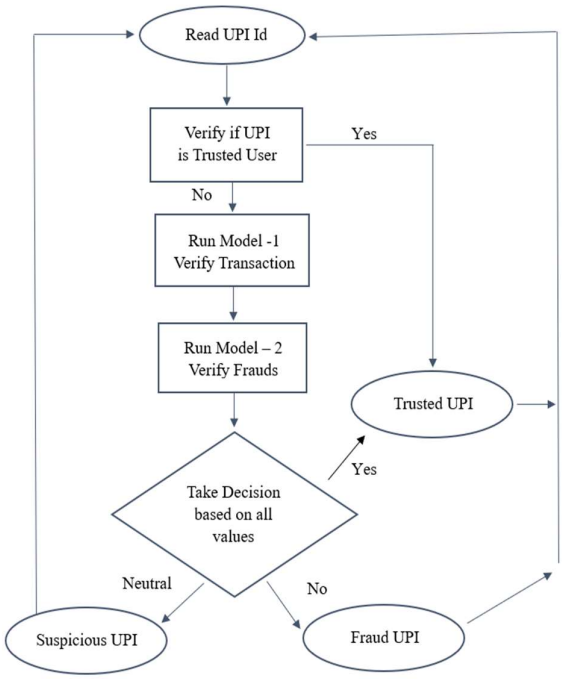

Fig. 2. Flow Chart

The fraud detection model evaluates the UPI ID using machine learning algorithms, primarily analyzing fraud patterns from bank statements. The detection process follows a priority-based approach:

- Priority 1 – The model analyzes past transaction patterns from the bank statement to identify any fraudulent activity.
- Priority 2 – It checks whether there are fraud reports associated with the UPI ID in previous transactions.
- Priority 3 – The system evaluates the account age (whether it is less than 30 days old) as newly created accounts are more prone to fraudulent activities.

The fraud detection model utilizes these priority values to analyze the overall risk profile associated with a given UPI ID, ultimately classifying it as either Safe, Suspicious, or Fraudulent. This analysis involves a sophisticated evaluation of various factors, each weighted according to its importance in indicating fraudulent activity. After processing this data, the model calculates a final risk score, providing a quantifiable measure of the potential threat. This score serves as the basis for a well-informed decision regarding the

security of the UPI ID. The determined fraud risk level, along with the calculated risk score, is then transmitted to the backend service. This service acts as a crucial intermediary, responsible for receiving the model's output, ensuring the correct risk category is assigned, and managing the presentation of the results to the user. The backend service dynamically populates the fraud risk value and seamlessly presents it to the user through the intuitive user interface. This immediate feedback mechanism ensures that users receive real-time insights into the safety and security of the UPI ID they have entered, empowering them to make informed decisions about their transactions. By seamlessly integrating real-time data processing, a priority-based evaluation system, and efficient backend communication, the SafeScan application delivers a reliable, intelligent, and proactive fraud detection mechanism. This comprehensive approach significantly enhances security, fosters trust in digital payments, and ultimately safeguards users from potential financial harm. The system's real-time nature allows for immediate action, preventing fraudulent transactions before they can be completed.

IV. Result Analysis

Table 1 presents the range of values used by the fraud detection model to determine the risk level of a UPI ID and decide the appropriate result to be displayed.

TABLE 1. RANGE FOR FRAUD DETECTION

Parameters	***Range***
Trusted	0-45
Suspicious	46-63
Fraud	64-100

Before the system goes live, carefully considered threshold values have been established to categorize UPI IDs based on the proportion of detected fraud patterns within their transaction history. These thresholds serve as critical boundaries for classifying UPI IDs into distinct risk categories, allowing for appropriate action to be taken. The classification system comprises the following categories and their corresponding thresholds:

1) Trusted: A UPI ID is classified as "Trusted" when the ratio of detected fraud patterns to the total number of transactions is less than 46%. This indicates a relatively low level of suspicious activity and suggests a lower risk profile.

2) Suspicious: A UPI ID is categorized as "Suspicious" when the ratio falls between 46% and 64%, inclusive. This range signifies a heightened level of potential risk, warranting further investigation and scrutiny. UPI IDs in this category may exhibit patterns that, while not definitively fraudulent, raise concerns and require closer monitoring.

3) Fraudulent: A UPI ID is deemed "Fraudulent" when the ratio of detected fraud patterns to total transactions exceeds 64%. This threshold indicates a high probability of fraudulent activity, requiring immediate action to mitigate potential losses and protect users. UPI IDs classified as fraudulent are likely to have exhibited clear patterns of abuse or unauthorized activity. These thresholds are designed to provide a clear and objective framework for assessing the risk associated with each UPI ID, enabling the system to prioritize its efforts and focus on the most pressing threats.

The degree of application and the outcomes are as follows.

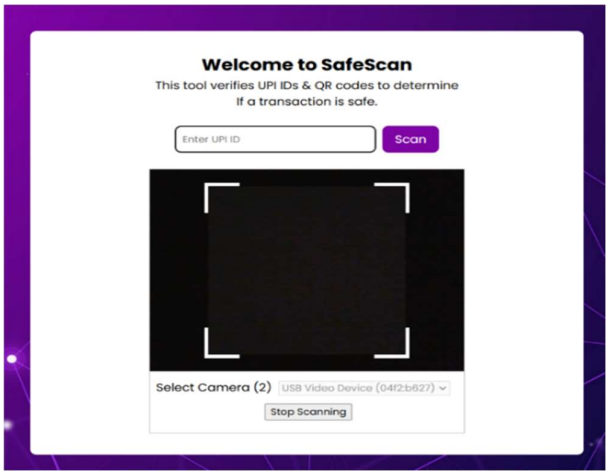

Fig. 3. Webpage Interface

Fig. 3. depicts the user input stage, where a UPI ID or valid UPI QR code must be provided. Upon submission, the web application first checks if the SafeScan database is loaded. If the database is not loaded, the user is redirected to an "Access Restricted" page (Fig. 4.). If the database is loaded, the application sends a request to the backend to verify the presence of the provided UPI ID in the database.

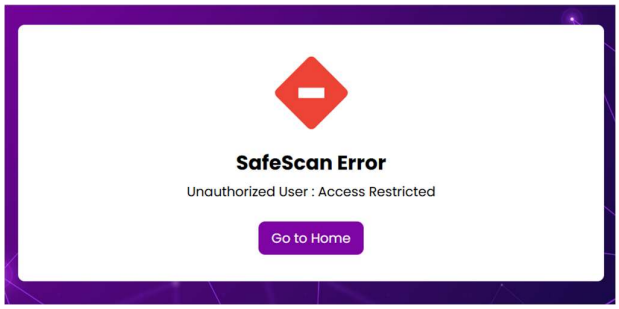

Fig. 4. Access Restricted Webpage Interface

Upon locating a UPI ID in the database, the application retrieves the data required for validation. If the UPI ID's status is already "Trusted" within the database, this status is immediately displayed to the user, bypassing further checks. However, if the UPI ID is not pre-classified as "Trusted," the application initiates a more in-depth verification process.

The backend server then transmits the relevant data, such as transaction history, to a machine learning model. This model scrutinizes the data, identifying patterns indicative of fraudulent activity, and generates a percentage score reflecting the likelihood of fraud. This score is subsequently evaluated against a set of predefined thresholds (Table 1) to determine an initial classification: Fraudulent, Suspicious, or Trusted. This provides a data-driven risk assessment.

In parallel, a second machine learning model analyzes user-reported instances of fraud associated with each transaction in the provided history. This analysis yields another percentage, representing the proportion of transactions with reported fraud. This percentage undergoes a similar comparison with the same thresholds in Table 1, resulting in a second independent classification. This leverages community feedback to identify potential risks.

Finally, the system calculates the age of the UPI ID, specifically the time elapsed since its creation. This age is then compared against a separate set of thresholds (Table 2) to generate a third classification. This adds a temporal dimension to the risk assessment. The rationale is that newer UPI IDs may carry inherently higher risk due to limited transaction history.

TABLE 2. RANGE FOR AGE OF UPI ID

Parameters	***Range***
Trusted	> 180 days
Suspicious	30-180 days
Fraud	< 31 days

These three classifications (from the two models and the UPI ID age) are then combined to produce a final overall classification (Fraudulent, Suspicious, or Trusted), which is displayed on the webpage.

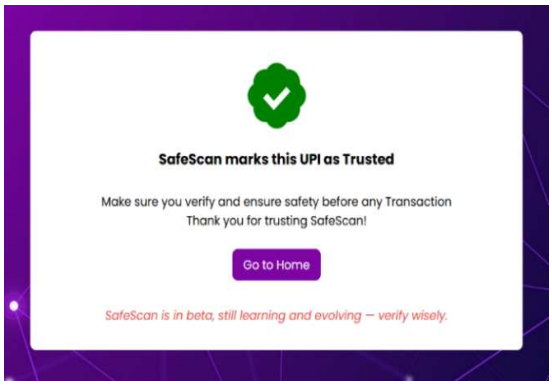

Fig. 5. Trusted UPI Interface

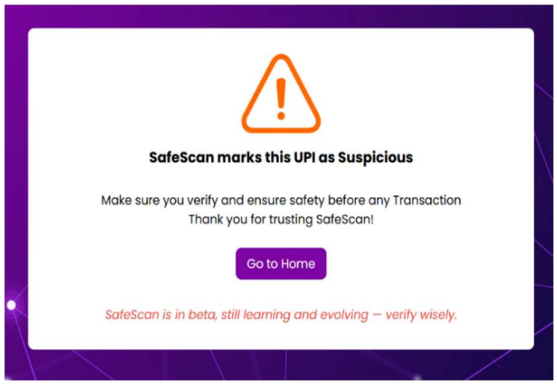

Fig. 6. Suspicious UPI Interface

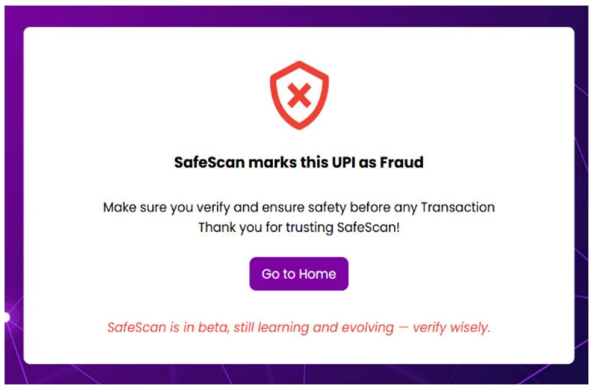

Fig. 7. Fraud UPI Interface

SafeScan, while robust, is subject to certain operational limitations. Several scenarios can lead to a failure in processing a UPI ID. For instance, if the provided UPI ID is not present in the SafeScan database, the application cannot proceed with verification. Similarly, if there is an issue retrieving the necessary bank statement data associated with a UPI ID – perhaps due to a temporary outage at the bank's end or an error in accessing the data – the system cannot complete its analysis. Other potential issues, such as internal system errors or data corruption, can also hinder the process. In any of these failure scenarios, where the system is unable to process the UPI ID, the application will gracefully display an "UPI Unavailable" screen, as shown in Fig. 8. informing the user of the issue and preventing unexpected application behavior. This ensures a consistent user experience even in the face of unforeseen problems.

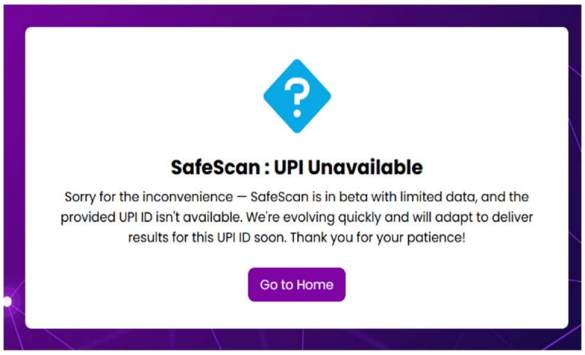

Fig. 8. UPI Unavailable Interface

CONCLUSION

SafeScan represents a paradigm shift in fraud detection for digital payments, leveraging the dynamic capabilities of machine learning to deliver real-time analysis and proactive security. Unlike traditional rule-based systems, which often struggle to keep pace with evolving fraud tactics, SafeScan continuously learns and adapts. This inherent adaptability ensures its long-term effectiveness in mitigating financial risks. By seamlessly integrating QR code verification, UPI ID validation, and AI-driven anomaly detection, SafeScan establishes a robust, multi-layered security framework. This comprehensive approach significantly reduces the vulnerability of both users and financial institutions to fraudulent activities. The system's ability to detect suspicious

transactions in real-time and provide instant results to users fosters greater transparency and builds trust in the digital payment ecosystem. Furthermore, SafeScan's inherent scalability allows for seamless integration across a wide range of payment platforms, making digital transactions safer, more secure, and increasingly resilient against future fraud threats. Its proactive approach not only detects current threats but also anticipates and mitigates potential future vulnerabilities. Ultimately, SafeScan is poised to redefine the landscape of fraud prevention in digital payments, paving the way for a more secure, reliable, and trustworthy financial ecosystem for all stakeholders. It empowers users with greater control over their financial security while simultaneously providing institutions with the tools they need to protect their systems and reputation.

FUTURE SCOPE

The future scope of SafeScan is vast, with significant improvements possible through advancements in technology and evolving fraud detection strategies. As fraud techniques become more sophisticated, our system will integrate enhanced security mechanisms and machine learning models to detect fraudulent activities more effectively. By leveraging AI-driven anomaly detection and behavioral analysis, SafeScan will proactively identify unusual transaction patterns and adapt to emerging fraud trends in real-time. Automation will play a crucial role in reducing human intervention and improving efficiency. Currently, the initial verification of UPI IDs involves manual effort, but future iterations will introduce automated validation, significantly reducing processing time and human workload. Additionally, our system will evolve to process transaction statements in real-time, using AI to flag suspicious activities instantly and make fraud detection more responsive. To support large-scale deployment, SafeScan will focus on improving its speed and scalability. Future developments will optimize machine learning algorithms for high-speed fraud detection, ensuring seamless analysis of vast amounts of financial data. By leveraging cloud-based infrastructure, the system will be capable of handling city-wide or even nationwide implementations. Furthermore, predictive analytics will be integrated to anticipate potential fraud patterns and mitigate risks before they occur. By continuously evolving with new security enhancements, automation, and high-performance computing, SafeScan aims to revolutionize digital fraud detection, making financial transactions safer, faster, and more secure.

REFERENCES

[1] A Survey of Credit Card Fraud Detection Techniques: Data and Technique Oriented Perspective - Samaneh Sorournejad, Zojah, Atani et.al - November 2016.

[2] Ruttala Sailusha ; V. Gnaneswar ; R. Ramesh ; G. Ramakoteswara Rao ,"UPI Fraud Detection Using Machine Learning ",2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS) ,19 June 2020.

[3] Solving the False positives problem in fraud prediction using automated feature engineering - Wedge, Canter, Rubio et.al - October 2017.

[4] PayPal Inc. Quarterly results - https://www.paypal.com/stories/us/paypalreports-third-quarter-2018-results.

[5] A Model for Rule Based Fraud Detection in Telecommunications - Rajani, Padmavathamma - IJERT - 2012.

[6] Hunt R. (2001). Pki and digital certification infrastructure, in Proceedings. Ninth IEEE International Conference on Networks, ICON 2001. pp. 234–239.

[7] Chatterjee D. A. and Thomas R. (2017). Unified payment interface (upi): A catalyst tool supporting digitalization – utility, prospects and issues, International Journal of Innovative Research and Advanced Studies (IJIRAS), vol. 4, no. 2, pp. 192–195.

[8] Pratyush Sharma, Souradeep Banerjee, Devyanshi Tiwari, and Jagdish Chandra Patni, "ML Model for UPI Fraud Detection - A Comparative Analysis", The International Arab Journal of Information Technology, Vol. 18, No. 6, November 2021 , pp 789-790.

[9] Scikit learn - machine learning library - http://scikit-learn.org.

[10] Dataset For Fraud Detection - https://www.kaggle.com/datasets/rupakroy/online-payments-fraud-detection-dataset.