RESEARCH ARTICLE OPEN ACCESS

Credit Card Fraud Detection

Mrs. Hemapriya B C[1], N G Manoj[2] ,Sahana H D[2] , Sanvi B N[2], Usha Rani C[2]

[1] (Department of Computer Science and Engineering, R.J Jalappa Institute of Technology, Bangalore Rural
Email: hemapriyacse@rljit.in)

[2] (Department of Computer Science and Engineering, R J Jalappa Institute of Technology, Bangalore Rural
Email: sudeepsudee696@gmail.com)

[3] (Department of Computer Science and Engineering, R J Jalappa Institute of Technology, Bangalore Rural
Email: sahana4599@gmail.com)

[4] (Department of Computer Science and Engineering, R J Jalappa Institute of Technology, Bangalore Rural
Email:sanvivokkaliga02@gmail.com)

[5] (Department of Computer Science and Engineering, R J Jalappa Institute of Technology, Bangalore Rural
Email:raniyadav123789@gmail.com)

--************************----------------------------------

Abstract:

The widespread adoption of digital payment platforms has enhanced convenience but also increased the risk of fraud, unauthorized access, and financial loss. This study proposes a simplified, efficient, and secure framework to protect users during online financial transactions by continuously monitoring activities in real time using key parameters such as transaction amount, user behavior patterns, device identification, location consistency, and transaction frequency. Based on this analysis, transactions are classified as safe, suspicious, or high-risk, where legitimate transactions proceed normally, suspicious transactions require additional authentication, and high-risk transactions are immediately blocked to prevent potential losses. For high-value transfers, the system enforces identity verification through facial recognition, adding a strong biometric security layer with minimal user inconvenience. Additionally, the framework provides a user-friendly interface for transaction history tracking and alert notifications, along with administrative tools for auditing logs and identifying emerging fraud patterns. By emphasizing real-time detection and reducing false positives, the proposed system enhances digital payment security, ensures data integrity, and builds user confidence in online financial systems.

--************************----------------------------------

I. INTRODUCTION

Digital payment platforms have become an essential part of everyday financial activities, enabling users to send money, settle bills, and purchase goods through online banking services, mobile applications, and digital wallets. These technologies offer speed and convenience while reducing dependence on physical cash; however, they also introduce greater exposure to fraud and unauthorized access. As reliance on digital payments continues to grow, maintaining transaction security has become a critical issue for both consumers and service providers. Cyber attackers constantly develop new techniques to exploit system vulnerabilities and user behavior, increasing the complexity of security threats.

The rise in digital transactions has led to a corresponding increase in fraudulent activities, including illegal transfers, identity abuse, and account compromise. Fraudsters often exploit stolen credentials, unfamiliar devices, or abnormal transaction patterns to bypass security controls. Many existing fraud detection approaches depend on predefined rules or manual verification, which are often insufficient to detect evolving fraud strategies. Additionally, such methods may delay legitimate transactions or incorrectly flag genuine users, resulting in poor user experience and reduced trust.

To address these limitations, an advanced solution is required that can monitor transactions continuously and detect suspicious behavior in real time. Rather than relying solely on static rules, the system should analyze transaction history, user behavior patterns, device characteristics, and contextual information to accurately identify potential threats as they occur.

II. LITERATURE SURVEY

[1] Sharma et al.: This study investigated the direct correlation between the exponential growth of digital payment infrastructures and the concurrent rise in cyber-fraud incidents. Their research highlighted that while the accessibility of online financial platforms offers convenience, it has simultaneously transformed these platforms into lucrative targets for malicious actors. The authors identified prevalent fraudulent activities, such as account takeovers and fictitious transactions, concluding that robust, automated monitoring systems are essential to maintain transactional integrity.

[2] Kumar and Singh: Kumar and Singh evaluated the efficacy of conventional fraud detection mechanisms predominantly utilized by banking institutions. Their analysis revealed that legacy systems often rely on static, rule-based logic—such as geographical restrictions and fixed transaction caps—which are effective only against known threat patterns. The study argued that these rigid models lack the adaptability required to counter evolving fraud techniques, rendering them progressively ineffective over time.

[3] Patel et al.: Focusing on behavioral analytics, Patel et al. proposed a dynamic approach that leverages historical transaction data to identify anomalies. Their research demonstrated that legitimate users typically exhibit consistent spending habits, and deviations from these established baselines often signal fraudulent activity. By comparing real-time actions against historical profiles, their methodology significantly improved detection accuracy and minimized the incidence of false positives.

[4] Rao and Mehta: This research examined the operational bottlenecks associated with manual fraud verification processes. Rao and Mehta noted that relying on human intervention for verification introduces significant latency and increases operational costs. Furthermore, they highlighted that manual review workflows are ill-equipped to manage high-volume transaction environments, leading to delayed responses that inadvertently increase the window of opportunity for successful fraud.

[5] Verma et al.: Verma et al. emphasized the critical importance of synchronous, real-time monitoring in fraud prevention architectures. Their findings indicated that systems capable of analyzing transaction data instantaneously can interdict fraudulent attempts before the transfer is finalized. This proactive capability is vital for minimizing financial liability and preserving user confidence in digital payment ecosystems.

[6] Ahmed and Khan: In their study on authentication protocols, Ahmed and Khan argued that single-factor authentication methods, such as static passwords or One-Time Passwords (OTPs), are no longer sufficient. Their work highlighted vulnerabilities to social engineering attacks like phishing and SIM swapping. Consequently, they advocated for the integration of multi-layered verification steps, particularly for sensitive or high-value operations, to bolster security.

[7] Das et al.: Das et al. explored the integration of biometric technologies, specifically facial recognition, into payment gateways. Their research concluded that biometric verification offers a superior level of security compared to text-based credentials, especially for high-value transactions. The authors noted that this method effectively mitigates risks associated with impersonation and unauthorized account access by ensuring the physical presence of the legitimate account holder.

III. EXISTING SYSTEM

Contemporary digital payment infrastructures predominantly utilize static, rule-based logic and manual auditing protocols to identify fraudulent activities. In these environments, transactions are assessed against a set of rigid, predefined criteria, such as spending thresholds, geographical consistency, device fingerprinting, and frequency caps. Any activity that deviates from these fixed parameters is automatically flagged as suspicious. Once a transaction is flagged, it typically undergoes a manual review process conducted by security analysts. This reliance on human intervention creates significant operational bottlenecks, leading to increased processing latency, higher administrative costs, and delays in clearing legitimate transfers. Furthermore, the authentication mechanisms in these legacy systems are often limited to standard passwords and One-Time Passwords (OTPs). These methods have proven increasingly vulnerable to sophisticated social engineering attacks, including phishing, SIM swapping, and credential stuffing.

A critical flaw in current architectures is their reactive nature; fraud is frequently identified only after the transaction has been finalized, rendering real-time prevention and fund recovery nearly impossible. Additionally, the lack of behavioral analysis results in a high rate of false positives, where genuine users are blocked, causing frustration and eroding trust in the platform. As transaction volumes scale, these non-adaptive systems struggle to maintain efficiency, failing to evolve alongside modern fraud techniques.

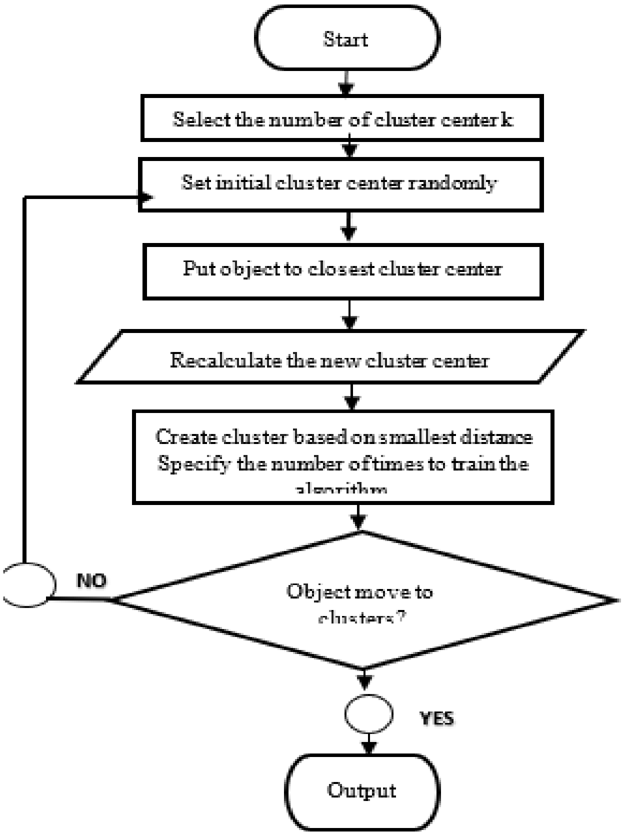

Start
Select the number of cluster center k
Set initial cluster center randomly
Put object to closest cluster center
Recalculate the new cluster center
Create cluster based on smallest distance
Specify the number of times to train the
algorithm
NO
Object move to
clusters?
YES
Output

Figure 1: Existing system

DISADVANTAGES OF EXISTING SYSTEM

1. **Static Detection Logic:** The reliance on fixed, heuristic rules renders the system ineffective against novel or adaptive fraud strategies. Attackers can easily circumvent these static parameters by slightly altering their techniques, leaving many sophisticated attacks undetected.
2. **Latency and Reactivity:** Most fraud is detected post-transaction. Because the system lacks robust real-time analysis capabilities, malicious transfers are often completed before intervention is possible, significantly increasing financial liability.
3. **Operational Scalability Issues:** The heavy dependence on manual verification limits the system's ability to scale. During peak traffic periods, the requirement for human review causes severe backlogs, slowing down system performance and increasing operational overhead.

4. **High False Positive Rates:** Strict, non-contextual rules often flag legitimate user activities as fraudulent. This results in unnecessary transaction denials, disrupting the user experience and diminishing customer satisfaction.
5. **Vulnerable Authentication:** reliance on basic 2FA (like SMS-based OTPs) exposes users to interception and account takeover attacks. The absence of biometric or behavioral verification layers makes unauthorized access significantly easier for attackers.
6. **Lack of Adaptability:** Legacy systems do not employ machine learning or adaptive mechanisms. Consequently, they fail to "learn" from historical fraud data, meaning the system does not improve over time and remains vulnerable to recurring attack patterns.

IV. PROPOSED SYSTEM

The proposed architecture addresses the structural deficiencies of legacy fraud detection frameworks by introducing a multi-layered, real-time security model. Unlike static systems that rely on rigid rules, this solution dynamically aggregates and analyzes transaction variables—including transfer magnitude, geolocation shifts, device fingerprints, and historical user patterns—as they occur.

By shifting to a holistic risk assessment model, the system categorizes transactions based on their calculated threat level rather than binary pass/fail conditions. This adaptive approach ensures that legitimate activities proceed without friction, while high-risk anomalies trigger immediate protective measures. To further harden security, the system incorporates step-up authentication mechanisms, such as biometric facial verification, specifically for high-value or suspicious requests. This methodology significantly reduces false positives and operational overhead, harmonizing robust security with a seamless user experience

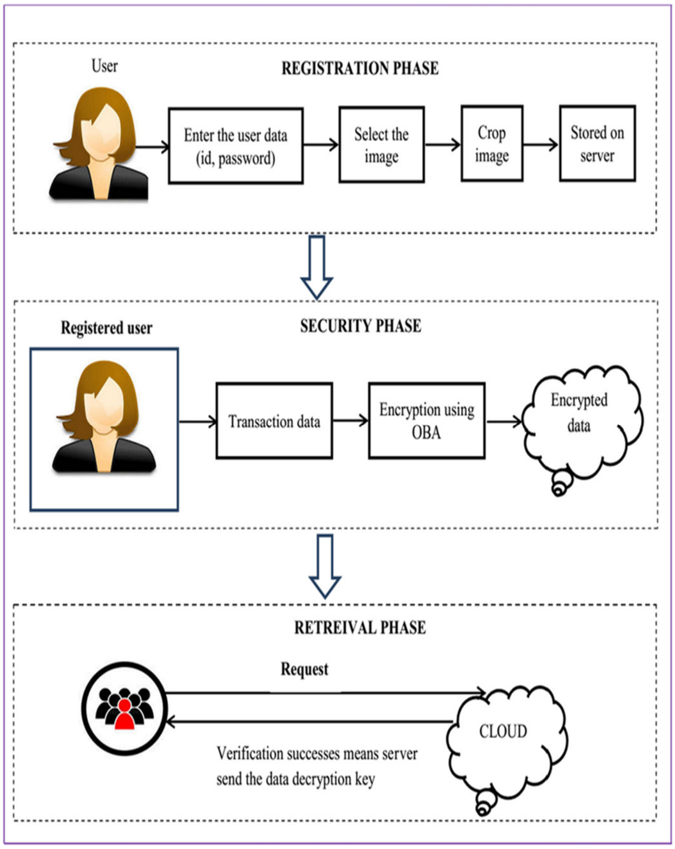


Figure 2: Proposed System

V. METHODOLOGY

The operational workflow is designed to detect and prevent fraud efficiently without disrupting genuine users. Upon the initiation of a financial transaction, the system instantly captures metadata, including timestamps, device identifiers, and geolocation. This data is cross-referenced in real-time against the user's established behavioral profile to identify anomalies.

The core logic utilizes a tiered risk classification engine:

Low-Risk: Transactions matching established patterns are authorized immediately to ensure seamless service.

Medium-Risk: Anomalies that do not pose an immediate critical threat trigger an intermediate verification step, requiring the user to confirm their identity via biometric checks.

High-Risk: Critical deviations or known threat indicators result in an automatic block to prevent financial liability.

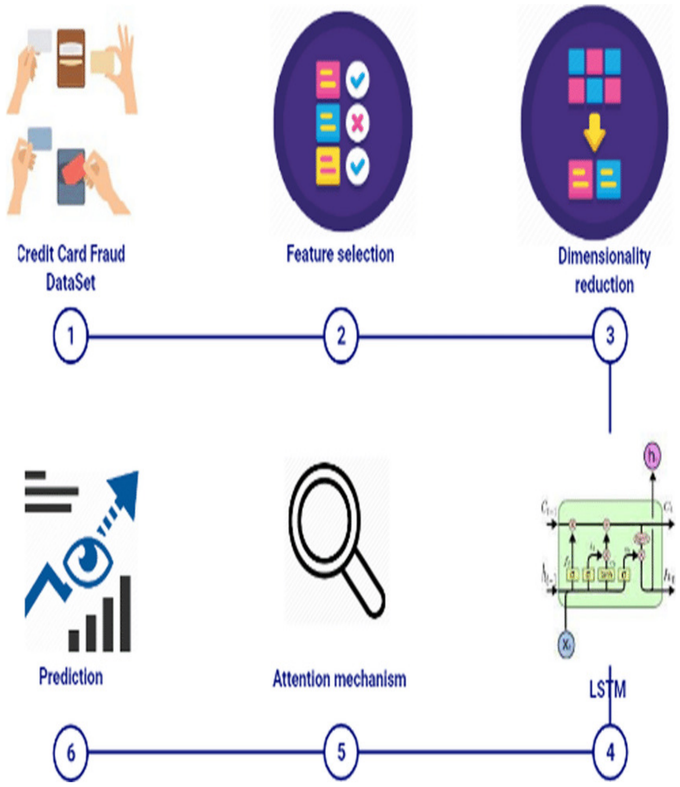


Figure 3: Architecture Diagram

A. MODULES (Same Sub-module Formatting)

1. User Authentication Module: This component manages secure access control via credential validation and OTP protocols. It ensures that only authorized entities can access the payment ecosystem, preventing unauthorized entry at the login stage.
2. Transaction Monitoring Module: This module executes continuous surveillance of transactional metadata (amount, time, location). By comparing current actions against standard user behavior, it identifies deviations and potential threats in real-time.
3. Risk Evaluation and Verification Module: Acting as the system's decision engine, this module classifies transactions into risk tiers (Low, Medium, High). It enforces the appropriate security response—approving safe transfers, challenging suspicious ones with step-up verification, or blocking high-risk attempts.
4. Alert and Reporting Module: This utility disseminates instant notifications to users regarding account activity and provides administrators with comprehensive logs. These records are essential for auditing system performance and analyzing emerging fraud trends.

B. ALGORITHM

The algorithmic process commences with user login and transaction initiation. The system simultaneously aggregates context data (location, device, history) and screens for anomalies. Based on this real-time analysis, a risk score is computed to classify the transaction.

- **If Low Risk:** Grant immediate approval.
- **If Medium Risk:** Trigger additional user verification (OTP/Face). * **If High Risk:** Execute automatic rejection to neutralize fraud before completion.

VI. RESULT

1. User Profile Creation: To initiate the secure onboarding process, the system enables new registrants to establish a protected profile by inputting fundamental identifiers, such as their legal name and mobile contact number. During this registration phase, the user is required to complete a facial verification step utilizing the device's integrated camera. This procedure authenticates the user's identity at the point of account origination. The biometric data captured is encrypted and securely linked to the user's profile, establishing a robust identity baseline that effectively prevents the creation of fraudulent or duplicate accounts by unauthorized entities.
2. Profile Verification and Storage: Upon the successful completion of the facial scan, the system executes a validation protocol to verify the accuracy and authenticity of all submitted data. Once validated, the user's profile information encompassing their contact details and biometric descriptors is archived within a secure database. Access to the login interface is restricted exclusively to users with fully verified profiles, a measure that eliminates the risk of fake accounts entering the ecosystem.
3. User Login: Registered participants access the platform by authenticating with their registered

phone number and secure credentials. A successful login event confirms the user's authorization to engage with the digital payment interface. This authentication gate ensures that only legitimate, verified individuals can initiate financial operations within the system.

4. Transaction Initiation: Post-authentication, the user commences a transfer by inputting necessary payment variables, including the transaction magnitude and recipient details. The system logs this request but places it in a temporary holding state. Processing is suspended until all subsequent security protocols are satisfied, preventing any premature transfer of funds without comprehensive verification.

5. OTP Verification: As the transaction progresses, the system generates a dynamic One-Time Password (OTP) and transmits it to the user's registered mobile device. The user is obligated to input this code within a defined expiration window. This step confirms physical possession of the registered device, adding a critical layer of multi-factor authentication to the process.

6. Face Verification During Transaction: Following successful OTP entry, the system triggers a live facial recognition challenge. The user's real-time image is captured via the device camera and instantly cross-referenced against the biometric data stored during registration. This biometric check ensures that the transaction is being authorized by the actual account holder, rather than an imposter who may have acquired the device and credentials.

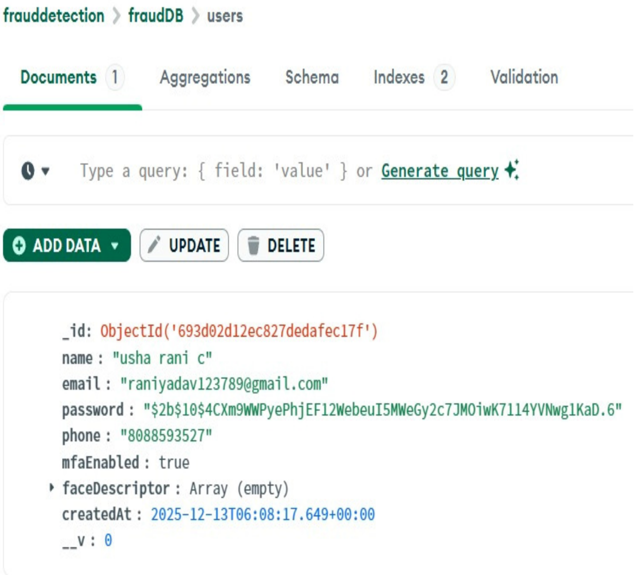
7. Verification Decision and Transaction Control: The system's decision engine simultaneously evaluates the outcomes of both the OTP entry and the facial scan. If both authentication factors are validated successfully, the transaction is approved and permitted to proceed. Conversely, if either the OTP is incorrect or the facial match fails, the system immediately terminates the transaction. This instantaneous blocking mechanism effectively neutralizes unauthorized access attempts and mitigates potential financial exposure.

8. Transaction Completion or Blocking: Transactions that pass all security checks are processed to completion without further latency. Blocked attempts are halted instantly, ensuring that funds remain secure until every security condition is met. This rigorous control framework maintains high standards of transaction safety and system reliability.

9. Alert and Notification: The system dispatches an immediate notification to the user, clearly stating the final status of the transaction (Approved or Blocked). These real-time alerts keep users apprised of account activity and enable them to react swiftly to any anomalous or suspicious events.

10. Result Storage and Monitoring: Comprehensive logs of every transaction including verification outcomes, precise timestamps, and the final decision (pass/fail) are securely retained in the system's database. These historical records provide administrators with the data necessary to audit user activity, analyze emerging behavioral patterns, and continuously refine the system's security logic.

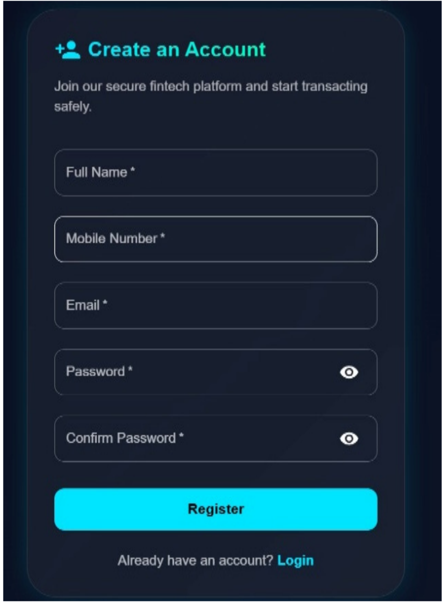
Description: A user record stored in the users collection of the fraudDB database contains a unique user ID along with essential details such as name, email, encrypted password, and phone number, which are required for secure login and OTP verification. The mfaEnabled field indicates that multi-factor authentication is enabled for the user, ensuring additional security during access and transactions. The faceDescriptor field stores face verification data used to confirm the user’s identity during sensitive actions. The createdAt field records the date and time of account creation, which helps in auditing and monitoring user activity. Overall, this structured record supports secure user management and strengthens fraud prevention in the credit card transaction system.


frauddetection > fraudDB > users
Documents 1
Aggregations
Schema
Indexes 2
Validation
Type a query: { field: 'value' } or Generate query
ADD DATA
UPDATE
DELETE

```
_id: ObjectId('693d02d12ec827dedafec17f')
name : "usha rani c"
email : "raniyadav123789@gmail.com"
password : "$2b$10$4CXm9WWPyePhjEF12WebeuI5MWeGy2c7JMOiwK7114YVNwg1KaD.6"
phone : "8088593527"
mfaEnabled : true
faceDescriptor : Array (empty)
createdAt : 2025-12-13T06:08:17.649+00:00
__v : 0
```

Figure 4: User Creation

Description: The user registration page of the credit card fraud detection system allows new users to create an account by entering details such as full name, mobile number, email, and password. The Register button submits the information to create the account, while the Login option is available for existing users. This simple and secure interface ensures proper user onboarding and acts as the first step in enabling further authentication methods such as OTP and face verification to enhance fraud prevention.

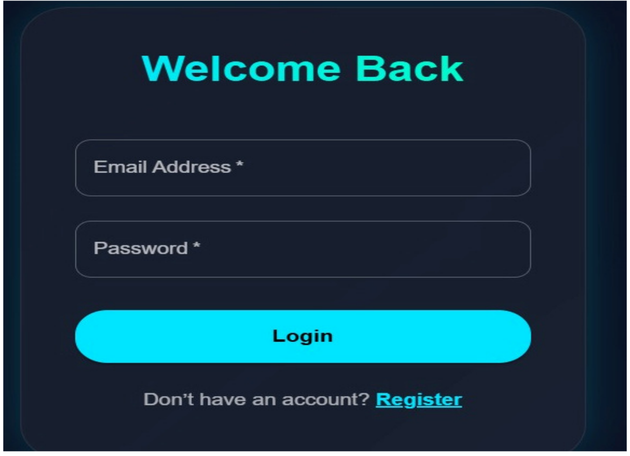


Create an Account

Join our secure fintech platform and start transacting safely.

Figure 5: Create an Account

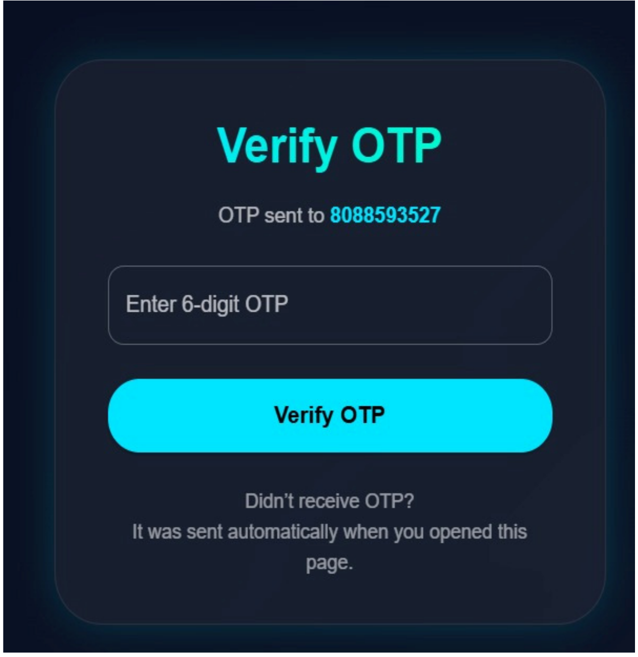
Description: The login page of the credit card fraud detection system, where registered users enter their email address and password to access the platform. The Login button verifies the user's credentials, while the Register option is available for new users. This page ensures secure access for authorized users only.



Welcome Back

Figure 6: Login Page

Description: The OTP verification page where a 6-digit OTP sent to the user's registered mobile number must be entered. Clicking the **Verify OTP** button confirms the user's identity and adds an extra layer of security to prevent unauthorized access.



Verify OTP

OTP sent to 8088593527

Didn't receive OTP?
It was sent automatically when you opened this page.

Figure 7: Verify OTP

Description: The image shows the face verification page where the user clicks Verify Face to scan their face using the device camera. The system matches the captured face with stored data to confirm the user's identity and prevent fraud.

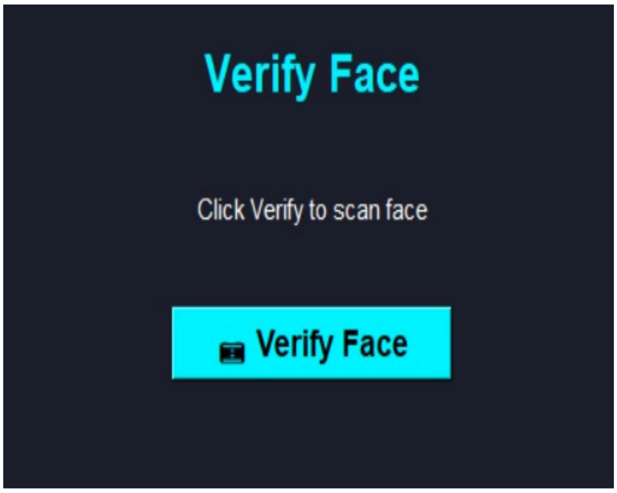


Figure 8: Verify Face

VII. CONCLUSION

This research successfully formulated and deployed a robust framework for detecting credit card fraud within digital payment ecosystems. By synthesizing multi-factor authentication protocols specifically integrating mobile-based OTPs with biometric facial recognition the system establishes a rigorous security perimeter that effectively negates unauthorized access. Unlike conventional models that depend heavily on static, rule-based logic or reactive manual audits, this proposed architecture emphasizes proactive, real-time intervention.

The integration of biometric validation provides a distinct advantage, rendering stolen credentials useless in the absence of the physical user. Consequently, this dual-layer verification strategy balances high level security with operational efficiency, ensuring that legitimate transactions are processed seamlessly while anomalies are instantly neutralized. Ultimately, this project demonstrates that a hybrid approach to authentication not only significantly mitigates financial risk but also restores and strengthens user confidence in digital financial platforms.

VIII. FUTURE DIRECTIONS

While the current system offers substantial improvements over legacy methods, future iterations will focus on optimizing the algorithmic precision of the authentication modules. Strategic enhancements include:

Scalability and Performance: As transaction volumes scale, the architecture will be refined to support high-concurrency environments, ensuring latency remains minimal during peak loads.

Advanced Behavioral Analytics: Future work will incorporate longitudinal data analysis to better understand complex user habits over extended periods, thereby improving the system's ability to distinguish between genuine behavioral shifts and fraud.

Cross-Platform Integration: Expanding compatibility to function across diverse payment gateways and banking applications will be a priority to facilitate real-world commercial deployment. **Heuristic Refinement:** Continuous updates to the detection logic will be implemented to reduce the rate of false positives further, ensuring a frictionless experience for valid users.

IX. ACKNOWLEDGEMENT

We would like to express our sincere gratitude to our project guide for their continuous guidance, valuable suggestions, and constant encouragement throughout the development of our project titled “Credit Card Fraud Detection System.” We are thankful to the Head of the Department and all faculty members for their academic support, technical assistance, and for providing the necessary resources and learning environment. We also acknowledge our institution for offering the infrastructure and facilities required to successfully carry out this project. We extend our heartfelt thanks to our friends and classmates for their cooperation and support during the project work. Finally, we are deeply grateful to our parents and family members for their constant motivation, patience, and moral support, which played a vital role in the successful completion of this project.

X. REFERENCES

[1] Dal Pozzolo, A., Bontempi, G., Snoeck, M., & Van den Poel, D. (2015): Adapting fraud detection systems to changing environments. *IEEE Intelligent*

Systems, 30(3) ,68–75. This study explains how fraud patterns change over time and why traditional rule-based systems fail to detect new fraud techniques. It highlights the need for adaptive and real-time fraud detection systems.

[2] Bahnsen, A. C., Aouada, D., & Ottersten, B. (2015): Cost-sensitive decision trees for fraud detection. *Expert Systems with Applications*, 42(19), 7361–7370.

The authors discuss how fraud detection systems should focus on reducing financial loss rather than only detecting fraud, emphasizing efficient decision-making during transactions.

[3] Whitrow, C., Hand, D. J., Juszczak, P., Weston, D., & Adams, N. (2009): Transaction aggregation as a strategy for credit card fraud detection. *Data Mining and Knowledge Discovery*, 18(1), 30–55. This research shows that analyzing transaction history and user behavior helps in identifying suspicious activities more accurately than single-transaction checks.

[4] Jain, A. K., Ross, A., & Prabhakar, S. (2004): An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 4–20. This paper provides an overview of biometric authentication methods and explains how face recognition improves identity verification and security.

[5] Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001): Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3), 614–634. The study discusses how biometric systems strengthen authentication and reduce the risk of impersonation and unauthorized access.

[6] Das, A., Dey, S., & Saha, S. (2018): Secure authentication using OTP and biometric verification. *International Journal of Computer Applications*, 179(34), 1–6. This paper explains how combining OTP with biometric verification improves transaction security and prevents unauthorized payments.

[7] Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012): The quest to replace passwords. *IEEE Security & Privacy*, 10(6), 44–51. The authors analyze the weaknesses of password-based systems and highlight the importance of multi-factor authentication for secure systems.

[8] Chaudhary, S., & Sharma, P. (2019): A review of fraud detection techniques in digital payment systems. *International Journal of Advanced Research in Computer Science*, 10(3), 45–50. This review summarizes existing fraud detection methods and identifies limitations of rule-based systems in modern digital payments.

[9] Li, S. Z., & Jain, A. K. (2011): Handbook of face recognition. *Springer*. This book provides detailed information on face recognition techniques and their application in secure authentication systems.

[10] Singh, R., Vatsa, M., & Noore, A. (2014): Face recognition with disguise and spoofing detection. *IEEE Transactions on Information Forensics and Security*, 9(2), 226–238. This research focuses on improving face verification reliability and preventing spoofing attacks, making it suitable for secure transaction authentication.