IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.154223

# A Context-Aware Security Layer for Preventing Account Takeover Attacks in Online Transactions

**N.punitha,ME.,[1] Omeshwar K[2], Poovarasan K[3], Sampath S[4], Shahul Hameed N[5]**

AP- AIDS, DSEC Perambalur Tamil Nadu India[1]

AIDS, DSEC Perambalur Tamil Nadu India[2-5]

***Abstract*—**The rapid growth of digital payment systems and e-commerce platforms has significantly improved convenience but has also led to an increase in online payment frauds and account takeover attacks. Traditional One-Time Password (OTP)-based authentication systems are vulnerable to social engineering attacks such as phishing, fake customer support calls, and deceptive messages. This paper proposes a contextaware security framework that enhances OTP-based authentication by integrating transaction details, location analysis, and real-time cybercrime reporting. The system links OTPs with billing information such as merchant name, transaction amount, and masked card details, enabling users to verify transactions before authorization. Additionally, the system detects suspicious activities using location-based anomaly detection and provides instant fraud reporting with transaction blocking. This approach transforms security from a reactive to a proactive model, reducing financial losses and improving user trust in digital payment systems.

***Keywords*—**OTP Security, Payment Fraud Detection, Context-Aware Authentication, Cybercrime Reporting, Ecommerce Security

## I. INTRODUCTION

### *A. Background and Context*

The widespread adoption of digital payments and ecommerce has revolutionized financial transactions. However, this growth has also increased vulnerabilities to cyber threats, particularly **account takeover attacks** and OTP-based fraud. Most online systems rely on OTP authentication, but attackers exploit users through phishing and social engineering. Current systems are **reactive**, detecting fraud only after transactions occur, leading to financial loss and delayed resolution. To address these limitations, a **proactive and user-centric security framework** is required that provides transaction transparency and real-time fraud prevention.support and remove the burden off human therapists are now necessary. While still very effective, traditional therapy is experiencing a growing demand that it simply can no longer keep pace with because of the inaccessibility, high cost and societal stigma around seeking help. These hurdles only reinforce the critical need for innovative approaches designed to support people with scalable and individualized mental health care.

### *B. Problem Statement*

Existing online payment systems primarily rely on One-Time Password (OTP) authentication as the main security mechanism, which creates a significant vulnerability in modern digital transactions. This dependence on OTP alone is insufficient, as cybercriminals can easily exploit users through phishing attacks, fake customer support calls, and social engineering techniques. Another major limitation is the lack of transaction context provided to users, such as merchant details, transaction amount, and location, making it difficult for them to verify the authenticity of a transaction before authorization. Additionally, fraud detection mechanisms in current systems are mostly reactive, identifying suspicious activities only after the transaction has been completed and financial loss has already occurred. This delay reduces the chances of preventing unauthorized transactions in real time. Furthermore, there is no integrated mechanism for instant cybercrime reporting within the transaction process, forcing users to manually report fraud after the damage is done. The absence of real-time alerts and transparency further weakens user confidence in digital payment systems. As a result, users remain highly vulnerable to OTP misuse and account takeover attacks. These shortcomings highlight the need for a more secure, proactive, and context-aware authentication system

  

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.154223

*C. Objectives*

**The main objectives of the proposed system are:** • **To enhance OTP authentication using transactionaware verification**

This objective ensures that OTPs are linked with specific transaction details like amount and merchant information.

It prevents misuse by allowing users to verify whether the transaction is legitimate before entering the OTP.

- **To provide real-time billing details during OTP validation**
  The system displays complete billing information such as product details and transaction amount along with the OTP. This improves transparency and helps users make informed decisions before confirming payments.
- **To detect suspicious transactions using location analysis**
  The system analyzes the geographical location and device context of the transaction. Any unusual or unfamiliar location is flagged as suspicious, alerting the user in real time.
- **To enable instant cybercrime reporting and transaction blocking** A direct reporting link is provided to users for immediate complaint registration in case of fraud. The system can also temporarily block transactions to prevent unauthorized fund transfers.

*D. Significance of the Study*

The proposed system plays a significant role in enhancing the security of online payment systems by addressing the limitations of traditional OTP-based authentication. It introduces a context-aware verification mechanism that provides users with detailed transaction information, enabling them to make informed decisions before authorizing payments. This approach helps in reducing the risk of phishing attacks and OTP misuse, which are common causes of financial fraud. The integration of location-based analysis adds an additional layer of security by identifying suspicious activities in real time. Furthermore, the system promotes proactive fraud prevention by allowing users to detect and stop unauthorized transactions before completion. The inclusion of an instant cybercrime reporting feature improves response time and increases the chances of recovering lost funds. It also reduces the dependency on delayed and manual reporting processes. By enhancing transparency and user awareness, the system builds greater trust in digital payment platforms. The proposed solution contributes to the development of a more secure and usercentric e-commerce ecosystem. Overall, it represents a shift from reactive security measures to a proactive and preventive approach in handling online payment fraud.

## II .LITERATURE REVIEW

*A .OTP-Based Authentication for Online Transactions*

*One-Time Password (OTP) authentication is one of the most widely used security mechanisms in online payment systems due to its simplicity and effectiveness in verifying user identity. It ensures that only the registered user can authorize a transaction by entering a temporary code sent via SMS or email. However, as highlighted in the project report, OTP systems are increasingly vulnerable to phishing attacks and social engineering techniques where users are tricked into sharing OTPs. Cybercriminals exploit fake calls, fraudulent messages, and deceptive interfaces to obtain OTPs and complete unauthorized transactions. Additionally, OTP messages often lack transaction details, making it difficult for users to verify legitimacy. This limitation reduces the effectiveness of OTP as a standalone security solution. Therefore, enhancing OTP with contextual information becomes necessary. The literature suggests that OTP alone is no longer sufficient for modern cybersecurity threats. This creates a need for improved authentication mechanisms that provide better transparency and protection.*

*B. **Machine Learning-Based Fraud Detection Systems***

*Machine learning techniques have been widely used in detecting fraudulent transactions by analyzing user behavior, transaction patterns, and spending history. These systems can identify anomalies and flag suspicious transactions for further verification. As mentioned in the report, such approaches improve detection accuracy over time and are highly useful in large-scale financial systems. However, a major limitation is that these systems often detect fraud only after the transaction has been initiated or completed. This reactive nature reduces their effectiveness in preventing real-time*

  

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.154223

*financial loss. Moreover, machine learning models require large datasets and continuous training to maintain accuracy. They also operate mostly on the bank's backend, without involving the user in the verification process. This lack of user interaction limits transparency. Hence, while machine learning enhances detection, it does not fully prevent fraud at the user level.*

***C. Location-Based and Multi-Factor Authentication Techniques*** *Location-based anomaly detection and multi-factor a uthentication (MFA) have been proposed to strengthen online transaction security. These techniques analyze the geographical location and device information of users to identify unusual access patterns. According to the report, such systems can detect suspicious login attempts when transactions originate from unfamiliar locations. MFA further improves security by combining multiple verification methods such as passwords, OTPs, and device authentication. While these methods increase protection, they also introduce complexity for users. Additionally, location-based systems alone are not sufficient, as attackers may bypass them using VPNs or spoofing techniques. Another limitation is that these systems do not provide transaction-specific context to the user. Despite improving authentication strength, they still lack integration with real-time fraud prevention and user awareness features.*

***D.Cybercrime Reporting and Secure Payment Frameworks***

*Cybercrime reporting systems and secure payment gateway architectures play a crucial role in handling digital payment frauds. Existing systems provide platforms where users can report fraudulent transactions after they occur. As discussed in the project report, these systems support investigation and legal processes but are often slow and manual. Reporting typically happens after financial loss, making them reactive rather than preventive. Secure payment gateways use encryption techniques to protect data transmission between users, merchants, and banks. While they ensure backend security, they do not address user-side vulnerabilities such as OTP misuse. There is also a lack of integration between transaction processes and reporting mechanisms. This gap delays response time and increases damage. Therefore, combining real-time reporting with transaction-level security is essential for effective fraud prevention.*

## *III. DATASET AND PREPROCESSING TECHNIQUES*

***A.Dataset Structure and Key Features***

*The dataset used in the proposed system consists of transactionrelated data collected during online purchases and payment processes. It includes user details such as user ID, email, phone number, and login credentials, along with transaction-specific information like product name, transaction amount, payment method, and billing details. Additionally, OTP-related data and timestamps are stored to track authentication activities. The dataset also captures location and device context to identify unusual access patterns. Each transaction is uniquely identified, enabling continuity in monitoring user behavior. The structured storage of order details, user information, and payment logs helps in analyzing transaction flows effectively. This dataset plays a crucial role in detecting suspicious activities and ensuring secure processing. By maintaining both user and transaction-level data, the system supports transparency and accountability. The collected data forms the foundation for fraud detection and reporting mechanisms.*

*B .Data Collection and Storage Mechanism*

The system collects data dynamically during user interactions such as registration, login, product purchase, and payment authorization. All user inputs, including billing and shipping details, are securely stored in a relational database (MySQL) as specified in the project report. Transaction data is captured at multiple stages, including cart addition, checkout, and OTP verification. The system also records email alerts, OTP generation logs, and fraud reporting activities. Data storage is designed to handle structured information such as user profiles, product details, and order history. Secure storage practices like password hashing and data encryption are implemented to protect sensitive information. The database maintains relationships between tables such as user, product, and order to ensure data consistency. Logging mechanisms are also used to maintain an audit trail for investigation purposes. This structured storage approach supports efficient retrieval and analysis of transaction data.

**C.Data Preprocessing And Security Measures**

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.154223

Before using the data for transaction verification and fraud detection, preprocessing techniques are applied to ensure consistency and reliability. User inputs are validated and formatted to avoid errors and inconsistencies during processing. Data normalization is performed to maintain uniformity across different modules such as authentication and payment systems. Sensitive information like passwords and transaction details is encrypted to enhance security. OTP data is time-bound and validated to prevent unauthorized reuse. The system also filters and monitors abnormal patterns such as repeated failed OTP attempts or unusual login locations. Session management techniques are used to track user activity and prevent session hijacking. Additionally, the system ensures that all transactionrelated data is properly linked and verified before approval. These preprocessing and security measures improve system accuracy, prevent vulnerabilities, and ensure safe handling of user data.

## IV.METHODOLOGY

### A. SYSTEM ARCHITECTURE DESIGN

The proposed system is designed using a modular architecture to ensure scalability, security, and efficient transaction handling. It consists of multiple components such as the user interface, application server, database, and security modules. The user interacts with the system through a web interface where actions like login, product selection, and payment initiation are performed. The application server processes these requests and communicates with the database to fetch or store data. Security modules such as OTP verification, email alerts, and fraud detection are integrated into the workflow. Each module operates independently but is interconnected for seamless functioning. The architecture ensures real-time data flow between components, enabling quick decision-making. It also supports logging and monitoring for audit purposes. This structured design improves reliability and enhances overall system performance. The modular approach also allows future integration of AI-based fraud detection.

### *B. User Authentication and Access Control*

*The system begins with a secure user authentication process to ensure that only authorized users can access the platform. During registration, users provide essential details such as name, email, phone number, and password, which are securely stored in the database. Passwords are encrypted using hashing techniques to prevent unauthorized access. During login, the system validates user credentials against stored records. If the credentials match, access is granted; otherwise, an error message is displayed. The system also includes mechanisms to prevent brute-force attacks by limiting repeated login attempts. Session management is implemented to maintain user activity and prevent session hijacking. This module acts as the first layer of defense against unauthorized access. It ensures data confidentiality and protects user accounts from misuse. Overall, authentication plays a critical role in maintaining system security.*

### *C. Context-Aware OTP Verification Process*

*The OTP verification process is enhanced by linking it with transaction-specific details such as product name, transaction amount, and billing information. When a user initiates a payment, the system generates a unique OTP and sends it along with transaction details via email or SMS. This allows the user to verify whether the transaction is legitimate before entering the OTP. The OTP is time-bound and expires after a short duration to prevent misuse. If the entered OTP matches the generated one, the transaction is approved; otherwise, it is rejected. The system also limits the number of OTP attempts to avoid brute-force attacks. By combining OTP with contextual information, the system improves transparency and reduces fraud risks. This approach ensures that users are actively involved in verifying transactions. It significantly enhances the security of online payments.*

### *D. Fraud Detection and Location Analys*

The system incorporates a fraud detection mechanism that analyzes transaction behavior and location data. It tracks the geographical location and device information from which the transaction is initiated. If a transaction originates from an unusual or unfamiliar location, it is flagged as suspicious. The system then alerts the user before proceeding with the transaction. This real-time analysis helps in identifying potential fraud attempts early. The system also monitors patterns such as repeated failed OTP attempts and abnormal transaction frequency. These indicators help in detecting malicious activities. By combining location analysis with behavioral monitoring, the system provides an additional layer of security. This proactive approach minimizes the chances of unauthorized transactions. It ensures that suspicious activities are detected and handled promptly.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.154223

### E. Fraud Reporting and Transaction Blocking Mechanism

The system provides an integrated fraud reporting feature that allows users to take immediate action in case of suspicious transactions. A security link is included in theemail notification sent during the transaction process. If the user identifies the transaction as fraudulent, they can click the link to report it instantly. This action redirects them to a cybercrime reporting platform where details are automatically populated. At the same time, the system can temporarily block the transaction to prevent fund transfer. Notifications are also sent to the bank and merchant for further action. All activities are logged to maintain an audit trail for investigation. This feature reduces response time and increases the chances of preventing financial loss. It bridges the gap between detection and action. Overall, it enhances the effectiveness of fraud management.

## V.SYSTEM ARCHITECTURE

### A. User Authentication Module

The User Authentication Module is responsible for verifying the identity of users before granting access to the system. It allows new users to register by providing basic details such as name, email, phone number, and password. These details are securely stored in the database with encryption techniques like password hashing. During login, the system validates the entered credentials with stored data. If the credentials are correct, the user is granted access; otherwise, an error is displayed. The module also includes protection against brute-force attacks by limiting repeated login attempts. Session management is implemented to track active users and prevent unauthorized access. It ensures that only authenticated users can perform transactions. This module acts as the first layer of security in the system. Overall, it safeguards user accounts and sensitive information.

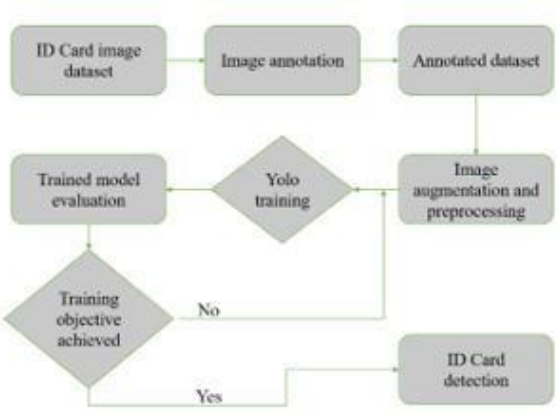


Fig 1:User Authentication Module

### B. Product Purchase Module

The Product Purchase Module enables users to browse, select, and purchase products securely. It displays products with details such as name, price, description, and availability. Users can add items to their cart and proceed to checkout. During checkout, billing and shipping details are collected. The system calculates the total cost, including taxes and delivery charges. Multiple payment options are provided to users for convenience. This module interacts with the OTP Verification Module to ensure secure payment processing. It ensures that all necessary data is captured before initiating a transaction. The module is designed for a smooth and user-friendly shopping experience. It plays a central role in handling ecommerce operations.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.154223

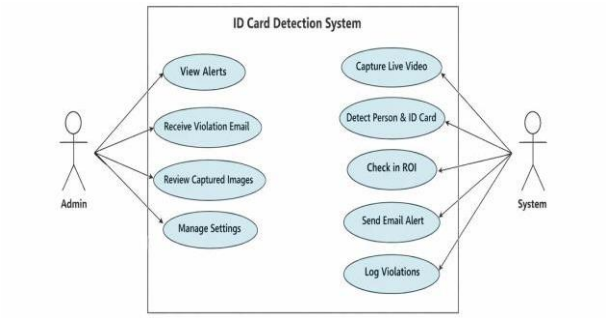


Fig2 :Use Case Diagram

### C. OTP Verification Module

The OTP Verification Module ensures secure transaction authentication using a one-time password. When a user initiates a payment, the system generates a unique OTP. This OTP is sent to the user's registered email or mobile number. The OTP is valid only for a short duration, enhancing security. The user must enter the OTP to confirm the transaction. If the OTP matches, the transaction proceeds; otherwise, it is rejected. The module limits the number of attempts to prevent brute-force attacks. It also links OTP with transaction details for better verification. This module provides two-factor authentication for enhanced security. It significantly reduces unauthorized transactions.

### D. Email Alert & Notification Module

This module sends real-time alerts to users during the transaction process. When a payment is initiated, an email is sent containing transaction details such as product name, amount, and billing information. This helps users verify whether the transaction is legitimate. The email also includes the OTP required for authentication. By providing detailed information, the system increases transparency. Users can identify suspicious activities before completing the transaction. This module acts as a warning system against fraud. It improves user awareness and decisionmaking. Notifications are delivered instantly to ensure timely action. Overall, it enhances the security and reliability of transactions.

### E. Fraud Reporting Module

The Fraud Reporting Module allows users to report suspicious or unauthorized transactions instantly. A security link is provided in the email notification sent during transactions. If the user detects fraud, they can click the link to report it immediately. This redirects them to a cybercrime reporting portal. The system can also trigger alerts to banks and merchants. In some cases, it temporarily blocks the transaction to prevent financial loss. All reported incidents are logged for investigation purposes. This module reduces response time and improves fraud handling efficiency. It empowers users to take quick action against cyber threats. Overall, it strengthens the system's security framework.

  

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.154223

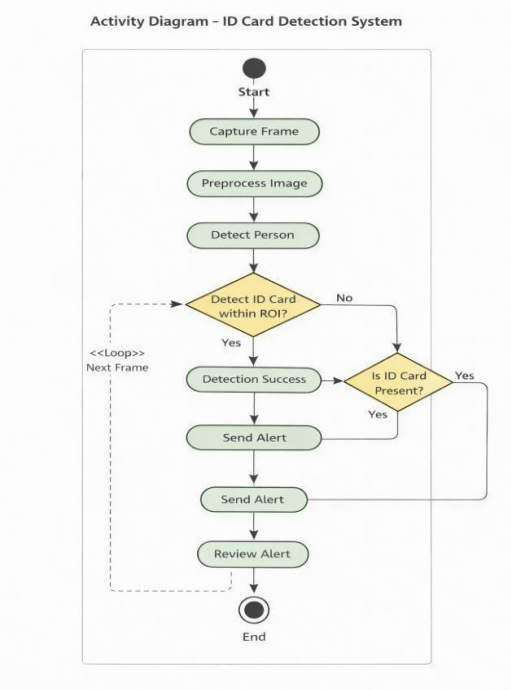


Fig 3: Fraud Reporting Module

F. Admin Monitoring Module

The Admin Monitoring Module provides control and oversight of the entire system. Administrators can view user details, transaction history, and system logs. It helps in identifying suspicious activities such as repeated failed OTP attempts. The admin can take actions like blocking users or investigating fraud cases. This module ensures smooth functioning of all system components. It also helps in maintaining data integrity and system performance. Logs are analyzed to detect patterns of cyber attacks. The admin can update system policies and security settings. It acts as a central control unit for managing the platform. Overall, it enhances system reliability and security.

## VI. RESULTS

### *A. System Performance and Accuracy*

*The proposed system was tested under multiple transaction scenarios to evaluate its performance and accuracy. The OTP verification process worked efficiently, ensuring that only valid users could complete transactions. The system successfully linked OTPs with transaction details, improving verification accuracy. Response time during authentication and payment processing was fast and reliable. The integration of modules such as authentication, OTP verification, and email alerts ensured smooth workflow execution. The system handled multiple user requests without performance degradation. Error rates were minimal, and incorrect transactions were effectively rejected. The database operations were consistent and secure during testing. Overall, the system demonstrated high accuracy in validating transactions. This confirms the effectiveness of the proposed architecture in real-time applications.*

### *B. Fraud Detection and Prevention Efficiency*

*The system showed strong performance in detecting and preventing fraudulent transactions. Location-based analysis successfully identified suspicious login attempts from unfamiliar regions. The email alert module helped users verify transaction details before entering OTPs, reducing phishing risks. In cases of suspicious activity, users were able to avoid sharing OTPs, preventing unauthorized access. The fraud reporting feature enabled immediate action, including reporting and blocking transactions. The system effectively minimized financial loss by stopping fraudulent activities in real time. Repeated invalid OTP attempts were detected and restricted automatically. The proactive approach improved overall system security. Compared to traditional systems, fraud detection was faster and more efficient. This demonstrates the advantage of integrating multiple security layers.*

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.154223

### *C. User Experience and System Reliability*

*User feedback indicated that the system was easy to use and highly reliable. The interface provided clear instructions during registration, login, and transaction processes. Users appreciated the detailed email alerts that included transaction information. This increased their confidence in verifying payments before authorization. The system provided smooth navigation and quick responses, enhancing user experience. The fraud reporting feature was found to be simple and effective. Users were able to take immediate action in case of suspicious transactions. The system maintained stability even during multiple operations. Overall, the proposed system improved user awareness and trust in digital payments. It delivered a secure and user-friendly experience.*

## VII . COMPARATIVE ANALYSIS

### A .Existing System vs Proposed System

The existing online payment systems mainly rely on OTPbased authentication without providing additional transaction context. This makes them vulnerable to phishing and social engineering attacks where users unknowingly share OTPs. In contrast, the proposed system enhances security by integrating OTP with transaction-aware details such as merchant name, amount, and billing information. Existing systems follow a reactive approach, detecting fraud only after the transaction is completed. However, the proposed system adopts a proactive approach by allowing users to verify transaction details before authorization. It also includes real-time email alerts that improve transparency. Unlike traditional systems, the proposed model enables instant fraud reporting and transaction blocking. The integration of multiple security layers improves reliability. The proposed system significantly reduces the chances of unauthorized transactions. Overall, it offers a more secure and user-centric solution compared to existing methods.

### B. Security Features Comparison

Traditional systems provide limited security features, mainly focusing on OTP verification as a second layer of authentication. These systems lack advanced mechanisms such as location-based analysis and contextual verification. The proposed system introduces multiple security layers including OTP with transaction details, email alerts, and location tracking. Existing systems do not provide real-time alerts with detailed billing information, which reduces user awareness. In contrast, the proposed system ensures that users are informed about every transaction detail before approval. It also detects suspicious activities using location-based anomaly detection. Fraud reporting in existing systems is manual and delayed, whereas the proposed system allows instant reporting and blocking. This reduces response time significantly. The combination of these features strengthens overall system security. Hence, the proposed system offers a more comprehensive security framework.

### C. Performance and User Experience Comparison

Existing systems often provide a basic user experience with limited interaction during the transaction process. Users are required to trust the system without sufficient verification information. This lack of transparency can lead to confusion and increased risk of fraud. The proposed system improves user experience by providing detailed transaction alerts and clear instructions. It enhances user awareness by involving them actively in the verification process. The system is designed to be user-friendly with smooth navigation and quick response times. Unlike traditional systems, it provides instant feedback in case of suspicious activities. The fraud reporting mechanism is simple and accessible, improving usability. Performance-wise, the system handles transactions efficiently without delays. It ensures both security and convenience for users. Overall, the proposed system delivers a better balance between security and usability.

## VIII . CONCLUSION

### A . Summary of the Proposed System

The proposed system presents a secure and efficient solution to address the limitations of traditional online payment authentication methods. It enhances the existing OTP-based mechanism by integrating transaction-aware verification,

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026
DOI: 10.17148/IJARCCE.2026.154223

which includes details such as merchant name, transaction amount, and billing information. This added context allows users to verify transactions before authorizing them, reducing the chances of fraud. The system also incorporates real-time email alerts that improve transparency during the payment process. Location-based analysis further strengthens security by identifying suspicious activities. The inclusion of an instant fraud reporting mechanism ensures quick response to cyber threats. All modules work together seamlessly to provide a reliable and user-friendly experience. The system shifts the focus from reactive to proactive security. It effectively minimizes risks associated with phishing and OTP misuse. Overall, it provides a comprehensive framework for secure digital transactions.

### B . Key Outcomes and Contributions

The implementation of the proposed system resulted in significant improvements in transaction security and user awareness. It successfully reduced the risk of unauthorized transactions by enabling users to verify details before entering OTPs. The fraud detection mechanism was able to identify suspicious activities in real time using location and behavior analysis. The instant reporting feature improved response time and helped in preventing financial loss. The system also enhanced transparency by providing detailed alerts during transactions. Users found the system easy to use and reliable, which increased their confidence in digital payments. Compared to existing systems, it offered better security features and faster fraud handling. The integration of multiple modules ensured smooth and efficient operation. This work contributes to the development of user-centric cybersecurity solutions. It demonstrates the effectiveness of combining authentication with contextual awareness.

### C. Future Scope and Improvements

Although the proposed system provides strong security features, there is scope for further enhancements. Future work can include the integration of artificial intelligence and machine learning techniques for advanced fraud detection. Biometric authentication methods such as fingerprint or facial recognition can be added for stronger identity verification. The system can also be expanded into a mobile application for better accessibility. Integration with banking systems and real-time fraud intelligence networks can improve coordination and response. Advanced behavioral analytics can be used to detect complex fraud patterns. Additionally, implementing multi-language support can improve usability for a wider audience. Continuous updates and security patches will ensure long-term reliability. The system can also be scaled to handle large volumes of transactions efficiently. These improvements will further strengthen the security and performance of the system. Overall, the future scope aims to make the system more intelligent and adaptive.

## REFERENCES

[1]. 1.G S. Gonzalez, A. Valenzuela, and J. Tapia, ‘‘Hybrid twostage architecture for tampering detection of chipless ID cards,’’ IEEE Trans. Biometrics, Behav., Identity Sci., vol. 3, no. 1, pp. 89–100, Jan. 2021.

[2]. H. Wang, S. Li, S. Cao, R. Yang, J. Zeng, Z. Qian, and X. Zhang, ‘‘On physicallyoccluded fake identity document detection,’’ in Proc. 31st ACM Int. Conf. Multimedia. New York, NY, USA: Association for Computing Machinery, Oct. 2023, p. 1556.

[3]. L. Zuo, W. Chen, Q. Hong, L. Huang, Z. Wang, and Y. Chen, “An intelligent knowledge extraction framework for recognizing identification information from real-world id card images,” IEEE Access 7, 2019.

[4]. Tropin, Daniil V. et al. “Improved algorithm of ID card detection by a priori knowledge of the document aspect ratio.” International Conference on Machine Vision (2021).

[5]. Pratama, M. Octaviano et al. “Indonesian ID Card Recognition using Convolutional Neural Networks.” 2018 5th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI) (2018): 178-181.

[6]. B Benalcazar, Daniel P. et al. “Synthetic ID Card Image Generation for Improving Presentation Attack Detection.” IEEE Transactions on Information Forensics and Security 18 (2022): 1814-1824

[7]. Satyawan, Wira et al. “Citizen Id Card Detection using Image Processing and Optical Character Recognition.” Journal of Physics: Conference Series 1235 (2019):.

[8]. Liem, Hoang Danh et al. “FVI: An End-to-end Vietnamese

[9]. Identification Card Detection and Recognition in Images.” 2018 5th NAFOSTED Conference on Information and Computer Science (NICS) (2018): 2022.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026
DOI: 10.17148/IJARCCE.2026.154223

[10]. Jian Zhu, Hanjie Ma, Jie Feng, Leiyan Dai; ID card number detection algorithm based on convolutional neural network. AIP Conference Proceedings 18 April 2018
[11]. 10 Sebastian Gonzalez; Andres Valenzuela; Juan Tapia, Hybrid Two-Stage Architecture for Tampering Detection of Chipless ID Cards, IEEE Transactions on Biometrics, Behavior, and Identity Science, 2637-6407, 2021.

[12]. 11.Reuben P. Markham; Juan M. Espín López; Mario NietoHidalgo; Juan E. Tapia, Open-Set: ID Card Presentation Attack Detection Using Neural Style Transfer, IEEE Access, 2169-3536, 2024.

[13]. 12.Ashwini Zinjurde and Vilas Kamble, "Credit Card Fraud Detection and Prevention by Face Recognition", International Conference on Smart Innovations in Design Environment Management Planning and Computing (ICSIDEMPC), 2020.

[14]. 13.Alharbi, F., Alshahrani, R., Zakariah, M., Aldweesh, A. and Alghamdi, A.A., 2023. YOLO and Blockchain Technology Applied to Intelligent Transportation License Plate Character
[15]. Recognition for Security. Computers, Materials & Continua, 77(3).

[16]. 14.Patil, S., Meshram, D., Bohra, M., Daulat, M., Manwatkar, A. and Gore, A., 2023, April. Enhancing Surveillance and Face Recognition with YOLO-Based Object Detection. In International Conference on Information and Communication Technology for Intelligent Systems (pp. 373-383). Singapore: Springer Nature Singapore.
[17]. 15.Haque, M., Faisal, S.M., Islam, M.T. and Akash, T.H., 2023.
[18]. Computer Vision-Based Intelligent Classroom Systems for Efficient
[19]. Power Management in Large Educational Institutions

  