IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, June 2026
Impact Factor: 8.2

Strengthening Security in Digital Payment Systems through Multi-Layered Authentication and Fraud Detection Mechanisms

Ishwar Patil
Department Of Computer Application, JSPM University, Pune, India

Abstract: *Digital payment systems have been changing how money moves around by giving users convenient, fast, and flexible options for making payments or transfers to one another. Fast growth in the use of mobile banking, online payment systems, and digital wallets has also resulted in an increase in the amount of financial fraud and cyber threats (e.g., cybercriminal attempts to hack bank accounts or steal money). Traditional methods of confirming users' identity such as passwords, PINs, and one-time passwords (OTPs) are being attacked and compromised by advanced methods like phishing, social engineering, and identity theft. Although many machine-learning-based systems have been developed for detecting fraudulent transactions in financial institutions, virtually all existing approaches treat the authentication and fraud detection process as separate entities. This division creates weaknesses in the security of the Digital Payment System infrastructure. This research proposes a security framework consisting of four layers that combines MFA, Device Authentication, Behavioural analytics data, and real-time machine-learning fraud detection in order to provide complete protection from unauthorized access and fraudulent financial transactions. Testing shows improved accuracy of detecting fraudulent activity by integrating fraud detection systems with authentication methods; increased security of digital payment systems through integrated security components.*

Keywords: Safe digital payments, Multi-step login security, Fraud detection, Device verification, User behaviour tracking, Real-time monitoring, Identity protection, Layered security system, Transaction risk analysis

I. INTRODUCTION

Modern financial ecosystems have been transformed by the implementation of digital payment systems that allow for fast, convenient and efficient financial transactions on a global scale. Mobile wallets, internet banking, contactless payment systems and peer-to-peer (P2P) applications are all examples of how the way both individuals and businesses perform financial transactions has changed. With the pervasive use of smartphones, access to the internet and FinTech innovations, the global adoption of digital payments has been accelerated. As a result, governments and financial institutions are encouraging the use of digital payment systems in order to promote financial inclusion, lower operational expenses and decrease dependence on cash.[1]

While digital payment systems offer advantages to consumers and businesses, their rapid implementation has also created new and different cyber security challenges for financial institutions. Digital payment infrastructures are very appealing for cybercriminals because of their ability to process large volumes of financial transactions, as well as store sensitive and private data pertaining to consumers. Cybercriminals use various methods to gain access to the vulnerabilities of payment systems, including phishing attacks, identity theft, malware injection, man-in-the-middle attacks and account takeover fraud. According to the cybersecurity report recently released, there has been an uptick in

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, June 2026
Impact Factor: 8.2

the number of incidents of financial fraud associated with digital payment systems over the last ten years, resulting in billions in financial losses for the institutions that process these transactions and for the consumers that use them.[3]

The traditional forms of authentication used in digital payment systems primarily consist of using passwords, PINs (or personal identification numbers), and OTPs (or one-time passwords). Although they have provided some level of basic security for many years, these types of authentication systems (or mechanisms) are becoming increasingly vulnerable to ever evolving cybercrime threats and vulnerabilities. An example of this is how phishers are able to trick unwitting users into disclosing their authentication credentials and SIM-swap attacks are allowing criminals to intercept mobile-based OTPs used to complete key payment transactions [4]. Therefore, just using traditional forms of authentication will no longer effectively protect any modern digital cash payment systems.

To combat these issues, financial institutions are now employing more and more machine learning-based fraud detection systems that evaluate historic transaction data in order to identify suspicious transaction processing behaviours. Such machine learning algorithms include: decision trees, and neural networks through analysis of transaction behaviour patterns of financial transactions to identify anomalies within the financial data associated with these types of transactions [5]. These systems allow for real-time monitoring of financial transactions and, therefore, able to help reduce much of the fraud that can occur through digital payment transactions.

Despite the latest technological innovations in fraud detection, many current digital payment security systems separate authentication mechanisms from fraudulent transaction detection systems. For example, authentication systems fit directly into the transaction execution portion of a transaction (i.e. authentication when users log into the system or start a new transaction), while fraud detection systems review transaction activity once the user has been authenticated. This disconnected relationship provides attackers with an opportunity to exploit the lack of connectivity between these two security components if they successfully bypass the authentication mechanisms.

To address the increasing need for a more comprehensive security model, it is critical to develop a security architecture that integrates different types of authentication mechanisms with intelligent methods to identify and detect fraudulent transactions that occur at different phases of a digital transaction. The proposed research will develop a multi-layered security architecture that includes; (1) multiple authentication mechanisms, (2) device verification mechanisms, (3) behavioural monitoring mechanisms, and (4) machine learning-based fraud detection mechanisms to help secure digital payment systems.

Digital payment systems represent a critical element of today's financial ecosystem due to their ability to enable secure and efficient financial transactions using many types of digital channels and platforms. Some examples of the digital payments available today are: A. mobile wallets, B. online banking, C. credit/debit card payments, and D. Peer-to-peer (P2P) payments. As digital payment technologies continue to evolve and gain traction in day-to-day consumer transactions, they have also demonstrated significant benefits such as reducing transaction time, increasing transaction accessibility, and providing financial inclusion opportunities for consumers on a global scale.

Digital Payment Systems Have Challenges When Securing Interconnected Digital Payment Systems Through Their Complex Architectures Makes Secure Payment Technologies Challenging. Payment Gateways, Banking Networks, Merchant Platforms, And Mobile Payment Applications Are Just A Few Of The Many Components That Are Disparate Yet Interconnected That Form A Payment Processing Ecosystem. Increasingly, The Large Number Of Interconnections Creates Many Potential Attack Surfaces, Which Places Digital Payments In Greater Risk To Cyber Attacks And Financial Fraud [7].

To Protect The Ecosystem Of Digital Payment Applications, It Is Essential To Have Strong Authentication Methods, Secure Communication Protocols, As Well As Sophisticated Online Fraud Detectors Capable Of Monitoring Potentially Suspicious Transactions In Real Time.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, June 2026
Impact Factor: 8.2

A. Digital Payment Ecosystem

Digital payment systems utilize a large number of connected entities to facilitate financial transactions between consumers and merchants. Digital ecosystem entities all support secure transaction processing and authorization among themselves.

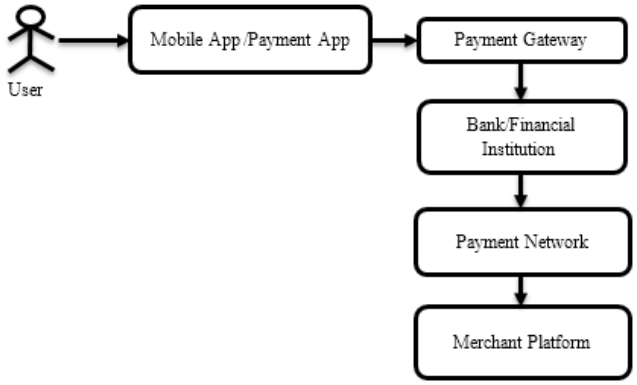

Fig. 1. Architecture of Digital Payment Ecosystem

The main elements of a standard digital payment ecosystem are:

- **Payment Service Providers (PSPs):**
  PSPs serve as intermediaries to facilitate payment processing and authorization for the consumer, merchant, and financial institution.
- **Financial Institutions:**
  Financial institutions (banks) facilitate consumer account management, authenticate transactions, and facilitate transfers between accounts.
- **Merchant Platforms:**
  Merchants implement gateways for digital payments onto their platforms to facilitate payments from consumers.
- **User Mobile Applications:**
  Mobile applications provide consumers with secure access to digital payment provided via mobile wallets, banking apps, and payment platforms.
- **Payment Processing Networks:**
  Payment processing networks (e.g., card networks and clearing house networks) facilitate the communication between financial institutions and settlement of successful transactions.

Secure communication between these components is vital to preventing fraud and to ensuring the integrity of transactions due to the complex digital infrastructure of all of the components [8].

B. Security Challenges in Digital Payments

Digital payment technology has many advantages, but it is also subject to many cybersecurity challenges that may compromise financial security and users' privacy.

1. Increased Volume of Online Financial Transactions

The rapid expansion of e-commerce and mobile banking has greatly increased the number of electronic financial transactions taking place on a global scale. This increase in transaction volume provides more opportunities for attackers to take advantage of vulnerabilities in electronic payment systems.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, June 2026 Impact Factor: 8.2

2. Increasingly Sophisticated Cyber-Attacks Against Financial Institutions

Cybercriminals are constantly developing new and advanced methods for attacking financial systems, including phishing, malware, ransomware, and distributed denial of service (DDoS) attacks. All of these attacks can disrupt payment services and cause large financial losses.

3. Ineffective Authentication Mechanisms

The majority of digital payment systems still utilize conventional authentication solutions, such as passwords and OTP-based verification, to authenticate users. These conventional solutions can be bypassed using password theft, phishing, and sim-swapping, allowing attackers to access financial accounts without authorization.

4. A Lack of Effective Real-Time Fraud Detection

Many electronic payment systems do not possess the necessary tools for real-time transactional monitoring, resulting in delays in detecting suspicious transactions while in process. Delayed detection of fraud increases the chance of financial loss and reduces the effectiveness of fraud prevention measures.

The single greatest vulnerability for digital payment systems is humans. Social engineering attacks take advantage of humans to trick them into giving up sensitive information such as user names and passwords or bank account information. Social engineering attacks rely on exploiting human trust rather than on exploiting technical vulnerabilities [13].

The combination of these security challenges demands an immediate need for advanced digital payment security architectures that have multiple layers of protection. The introduction and use of multi-layer authentication processes, combined with advanced fraud detection systems, dramatically improve the ability of digital payment systems to withstand the continuing evolution of cyber threats.

III. RELATED WORK

Many researchers propose various ways to make digital payment systems more secure; however, these efforts can generally be divided into two categories: (A) Authentication Mechanisms and (B) Fraud Detection Mechanisms (or other types of fraud detection).

(A) Authentication Mechanisms

Multi-Factor Authentication (MFA):

Many Digital Payments systems now use some form of MFA (multi-factor authentication) as a way to increase the security of their digital payments before letting customers access these funds by providing the user with two or more verification methods that confirm an individual's identity, including: passwords, biometric scans (when applicable), and verification through the device being used to check the account.

There are a number of studies that demonstrate the effectiveness of multi-factor authentication in reducing identity theft and unauthorized access to customer accounts that use Digital Payments [1].

Biometrics (such as fingerprint, facial recognition and iris scanning) are also beginning to be included in some mobile banking applications to assist in creating more secure digital payment systems [2].

The majority of digital payment systems currently use one-time passwords (OTPs) as their primary Authentication Mechanism, which can still be exposed to attack through phishing attacks or SIM-swapping fraud.

(B) Fraud Detection Through Machine Learning:

There has been a great deal of research conducted on machine learning algorithms for the purpose of detecting fraudulent financial transactions. The basis for machine learning applications to identify fraudulent financial transactions is that the algorithms review each of the financial transaction(s) of a financial institution, as well as patterns of fraudulent activity associated with other financial institutions, to create an anomaly variable for the algorithms that will then alert the algorithm to trigger fraud alerts.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, June 2026 Impact Factor: 8.2

Algorithms such as Random Forest, Support Vector Machines and Neural Networks have all been frequently applied in financial fraud detection applications [3]. In addition, many organizations have researched ways of using emerging Deep Learning techniques to identify complex fraudulent behaviours within large amounts of transaction data [4]. While most Fraud Detection Machine Learning Models are extremely accurate, they are generally implemented independently of any authentication methods.

C. Behavioural Biometrics as an additional layer of security in Finance.

Behavioural Biometric Technology is the continuous analysis of an individual's pattern of behaviour when interacting with online systems, including input methods such as typing speed and accuracy, devices used to access a system, and any habitual or typical transactional activity. Studies show that incorporating Behavioural Biometrics as part of Fraud Detection will improve accuracy by allowing the identification of legitimate users or customers from potentially fraudulent user behaviour [5]. Nevertheless, Behavioural Analysis is not commonly applied as part of an authentication framework within Digital Payment Systems.

IV. RESEARCH GAP

A lot of studies have recently looked at security solutions for digital payment systems, primarily focusing on authentication methods and fraud detection systems. Some common authentication methods have become popular - like multi-factor authentication (MFA), bio-metric authentication and one-time password (OTP) verification -all of which are being used to provide a higher level of identity verification on financial platforms [14]. In addition to this, many researchers are utilizing machine learning and AI-based solutions to detect potentially fraudulent transactions via pattern-related behaviour within financial datasets [15].

Unfortunately, the majority of approaches to this research treat authentication and fraud detection systems as independent security elements. Authentication systems are primarily concerned with authenticating the user when they log in/start a transaction, while the fraud detection component analyzes transaction patterns after the user has been successfully authenticated [16].

As a result, the way in which these two types of security systems are separated creates a significant security vulnerability. Should an attacker compromise an authentication framework using phishing, credentials being stolen or SIM swapping, they would have access to a user's account and could perform fraudulent transactions before any fraud detection system registered the suspicious activity [17]. Thus, the effectiveness of the fraud prevention systems is severely diminished.

Many current fraud detection systems depend purely on transactional data and fail to use contextual information like user behaviours, device identities or risk-based authentication signals. This lack of context limits the ability of these systems to detect complex fraud attacks in real time [18].

Another limitation in current research is that there is no well-developed security architecture that employs multiple layers of security – such as authentication mechanisms, behavioural biometrics, device verification technology and intelligent fraud detection models. Proposed solutions mostly improve single components of security rather than developing a comprehensive security architecture for digital payment systems [19].

Thus far, this research study has identified a primary research gap:

No integrated multi-layered authentication combined with real-time fraud detection framework to provide full protection to digital payments.

To fill this research gap, this research proposes a new type of multi-layered security architecture that integrates multi-factor authentication, device verification, behavioural monitoring and artificial intelligence based fraud detection. By integrating these security measures into one cohesive security framework, this approach will improve transaction security, increase the rate of successful identification of fraudulent transactions and improve the overall ability of digital payment systems to withstand new cyber threats.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, June 2026
Impact Factor: 8.2

V. PROPOSED MULTI-LAYER SECURITY FRAMEWORK

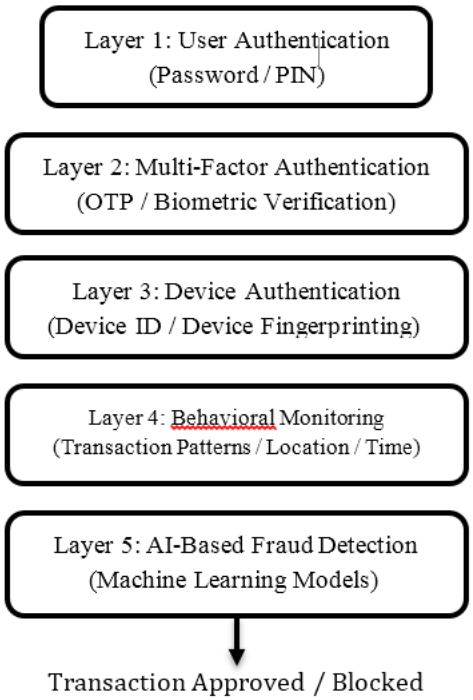

Fig. 2. Proposed multi-layer security framework for digital payment systems.

This study has proposed a multi-layered security framework in order to curb the existing limitations of current digital payment systems and implement an all-encompassing solution that integrates a variety of security measures, such as:

- Authentication and verification methods
- Device verification
- Behavior monitoring
- Real time fraud detection

The design of the proposed security framework is intended to offer a defense-in-depth approach to combating cyber threats and financial fraud.

Incidentally, most existing digital payment systems use only one or two layers of authentication to provide security and thus have proven to be inadequate to mitigate cyber-crime perpetrated through:

- Credential theft
- Phishing
- Account take-over attacks

The proposed multi-layered security framework is being introduced as a means of creating multiple layers of security that will provide a continuous, seamless means of verifying the user's identity and monitoring the transaction activity as it occurs during the digital payment process.

The use of a multi-layered structure will enable the user and all parties involved in the transaction to have peace of mind in knowing that even if one layer of security has been compromised, all other layers of security will be able to identify and stop instances of suspicious activity, as well as detect and prevent fraudulent transactions.

A. Layer 1: User Authentication

The foremost layer of security is verifying who the user is who is trying to access the digital payments system. Users verify who they are when they attempt to log onto the digital payments system by using traditional means of

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, June 2026 Impact Factor: 8.2

authentication (e.g., username and password, personal identification number or PIN, or secure login tokens). These means of authentication serve as the initial point of verification that grants users access to financial services. Traditional password authentication still remains the most commonly used method for verifying user credentials because it is easy and convenient; however, relying solely on password authentication can result in exposing the digital payment system to various types of risks, such as brute-force attacks, credential theft, and phishing attacks(the source of this information is found in [20]). therefore, the first security layer acts as a primary barrier to unauthorized users accessing the system but is not the only verification method that must support the identity verification process.

B. Layer 2: Multi-Factor Authentication

The second layer of security is multi-factor authentication (MFA). MFA is an enhanced method used to authenticate users through the verification of multiple factors in addition to their password. The most common forms of multi-factor authentication are as follows; (1) One-Time Passwords (OTP) - are temporary validation codes sent through SMS or authentication applications, (2) biometric authentication (i.e., fingerprint authentication, facial recognition, or iris scanning), and (3) a combination of hardware tokens (i.e., secure devices that generate an authentication code) and authentication applications. Having multiple forms of authentication significantly reduces the opportunity for a user to access the system without authorization, since an attacker must alter multiple authentication validation forms to gain access to the system. Studies show that MFA can reduce the likelihood of a successful cyberattack on a financial institution by a significant percentage.

C. Layer 3: Device Authentication

This layer confirms that a legitimate device has been used to initiate the transaction. Device Authentication guarantees that a transaction is being carried out using a trustworthy device related to the user's account.

Methods for verifying a device's identity include:

- Collecting a unique signature from each device
- Verifying the device's identification number
- Checking the IP address
- Profiling the device's browser and operating system

Device Fingerprinting obtains various characteristics of a user's devices (operating system, browser set-up, resolution, and the hardware used) so that those devices can be recognized as unique. When an Unidentified or Suspicious device initiates a transaction, the system can initiate additional authentication methods.

This layer can protect against Account Takeover attacks, where an attacker attempts to gain access to a user's account from a device that doesn't belong to the user.

D. Layer 4: Behavior Monitoring

The fourth layer monitors user behavior for the purpose of continuously tracking how users typically transact while engaging in computer-based transactions. Monitoring people's normal behaviors helps identify any activity that may be fraudulent in nature.

Some of the common behavioral characteristics being analyzed are:

- frequency of transactions
- the amount of transactions
- geographic location of transactions
- the times when transactions are conducted while signing on
- the devices that were used when conducting the transactions

For example, if a user usually uses the same geographic location to conduct his/her transactions and all of a sudden tries to conduct transactions from a different geographic location, the system would indicate that this is a sign of possibly fraudulent activity.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, June 2026 Impact Factor: 8.2

Behavioral biometrics also assist in preventing fraud through the analysing of how users behave, such as how users type and how they navigate around their devices [23].

E. Layer 5: AI-Based Fraud Detection

Layer 5 of the framework incorporates the use of machine-learning algorithms to detect fraud by identifying transactions that may be fraudulent (i.e., suspicious) in real-time. Fraud detection occurs through the analysis of large amounts of transactional data, such as:

- Amount of the transaction
- Location of the transaction
- Time of the transaction
- Device used in the transaction
- User behaviour patterns

If an anomaly/suspicious pattern is detected within a transaction(s), a block/flag would be generated to prevent the transaction from proceeding until further verification is performed or completed.

AI-based fraud detection provides a more effective solution for detecting fraud than traditional rule-based fraud detection systems, because they are capable of adjusting to fluctuations in patterns and are also capable of recognizing fraud patterns that are not yet established.

F. Framework Workflow

The multi-layer security framework outlined here has an overall workflow that consists of sequential verification steps as follows:

1. The digital payment application is first opened; then you enter in your login credentials.
2. Verification of your entered username/password occurs within the user authentication layer.
3 .If successful, the user undergoes multi-factor authentication via an OTP or biometric validation.
4. Device authentication verifies that the user is coming from a trusted device to submit their login request.
5. Behavioral monitoring examines the customer's historical transaction activity and patterns.
6. A fraud detection system that utilizes artificial intelligence evaluates the risk associated with this specific transaction.
7. If no indications of suspicious activity were detected, the transaction would be considered valid, and approval would be provided; however, if any indications of suspicious activity were detected, additional authentication will be required to validate the transaction, or the transaction will be blocked.

The layered methodology of the framework provides continuous validation and monitoring activities that strengthen the security of digital payment systems.

VI. METHODOLOGY

The methodology for this research utilizes structured methodological framework for both the design and evaluation of a multi-layer security framework for digital payment systems. The research methodology focuses on the use of authentication mechanisms, behavioral analysis, and machine-learning methods to help improve transaction security. The research methodology consists of multiple stages that include data collection, data preprocessing, feature engineering, model development, and model evaluation.

A: Data Collection

A major aspect of the experiment is collecting transaction datasets from digital payment platforms, which contain historical transaction records. The datasets used in this study contain transaction records of both legitimate and fraudulent transactions, making them valuable sources for developing and validating machine learning models for determining whether or not a transaction is fraudulent.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, June 2026
Impact Factor: 8.2

All datasets contain multiple important attributes for describing the details associated with each transaction, including: (1) total amount of the transaction, (2) physical location of the transaction, (3) when (time/date) the transaction took place, (4) information about the device used to initiate the transaction (i.e., device ID, operating system, browser), and (5) historical user behavior patterns related to the specific user (i.e., frequency of transactions, average purchasing amount, frequency of login sessions) for each transaction. These attributes can be used to derive insights into transaction patterns and identify potential transaction anomalies that may indicate a fraudulent transaction.

B. Preprocessing of Data

Before performing machine learning analysis, the transaction data needs to be processed to prepare a clean dataset from the raw transactions. Financial institution datasets in the real world typically contain records with incomplete, inconsistent, or noisy data that could hurt performance of a machine learning model. Therefore, preprocessing steps must be employed in order to provide uniform and reliable data.

The preprocessing steps in the dataset are as follows:

1. Cleaning the Data - Remove duplicate entries and correct inconsistencies in the data.

2. Filling in Missing Data - Use of statistical imputation methods like mean imputation or interpolation to address missing values.

3. Normalizing the Data - Numeric features like transaction amounts will be normalized to provide consistent value ranges within the dataset.

4. Encoding Data - Categorical attributes such as transaction type or merchant type will be converted into numerical form using encoding methods such as one-hot encoding.

The above preprocessing assist in developing a more accurate and efficient machine learning model.

C. Feature Engineering

Feature Engineering is the process of extracting / transforming relevant data attributes for the purpose of improving machine learning's ability to accurately predict. Utilizing adequate feature engineering techniques will assist machine learning algorithms in determining patterns and relationships that are not obvious (i.e., "hidden") within transaction data.

Some Examples of Engineered Features are outlined below:

- Transaction Frequency (i.e., how many transactions have been completed by a user during a designated/timeframe)
- Average Transaction Amount (i.e., what is the average dollar value of all purchases made by a user)
- Location Anomaly (i.e., by comparing historical user transaction data to today's 'current/location of transactions
- Device Usage Profile (i.e., frequency with which a user uses a certain type of device to make transactions)
- Time-Based Usage Profile (i.e., how often the user completes transactions during unusual hours; example: late-night hours)

All of these features may assist an algorithm in detecting anomalies, which could indicate a potential fraudster.

D. Model Development

In the model development phase of machine learning algorithms are developed to differentiate transactions into genuine or fraudulent transactions. Supervised learning is used as it requires previously classified transactions as patterns to train.

The algorithms developed as part of this project include:

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, June 2026 Impact Factor: 8.2

1. Logistic Regression Logistic Regression is a statistical method of classifying a transaction into either the fraudulent class or the legitimate class by studying characteristics of transactions in the historical data set to estimate the probability of fraud occurring. Logistic regression is an attractive model because of its simplicity and ability to describe the models to regulators and other stakeholders.
2. Random Forest Random Forest is an ensemble learning model that develops many decision trees for classifying transactions and averages their predictions to develop a final decision. Random Forest is particularly useful in the fraud detection application as it will be able to find many complex relationships between variables to make a better classification model.
3. Neural Networks Neural Network models are capable of learning many complex nonlinear relationships over large amounts of data. Neural networks are capable of identifying complex fraudulent activity such as identity theft that may not be identifiable using traditional statistical methods.
The models use historical transaction data for training and changes to the training process to enhance the model's performance in detecting frauds will take place.

E. Model Evaluation

The proposed fraud detection models' effectiveness will be evaluated using various performance metrics. These metrics are used to assess how well each model classifies transactions properly as being either fraudulent or legitimate.
Evaluation metrics include:
1. Accuracy
Accuracy is the percentage of transactions in the dataset classified correctly.
2. Precision
Precision is the ratio of the number of transactions that the model predicted to be fraud relative to the number of transactions that were predicted as fraud by the model.
3. Recall
Recall is a measure of how well the model identified transactions that were actually fraudulent.
4. F1 Score
F1 Score is an average of both precision and recall that can be particularly helpful when testing models on imbalanced data sets such as those frequently encountered in fraud detection.
Using these evaluation metrics will give a complete evaluation of each models' performance and their ability to fulfill the objectives of the proposed security framework.

VII. FINDINGS AND DISCUSSION

This section reports the results of evaluating the multi-layer security framework designed for securing digital payment systems. Effectiveness was assessed through the integration of multi-factor authentication mechanisms with device verification mechanisms, as well as the use of behavioral monitoring tools and machine-learning-based models for detecting fraud based on data obtained from transaction efforts.
The experimental results show that the new framework provides much higher levels of security in transactions and greater accuracy of detecting fraud compared to using a single-layer authentication system.
The machine-learning models designed in this work were created using historical datasets of digital payment transactions that had both legitimate and fraudulent transactions. Model performance was measured through standard measures including precision, recall, F1 score, and accuracy.
The results indicate that using multi-layered security substantially improves the ability of a system to identify fraud and simultaneously maintain secure authentication for legitimate users.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, June 2026
Impact Factor: 8.2

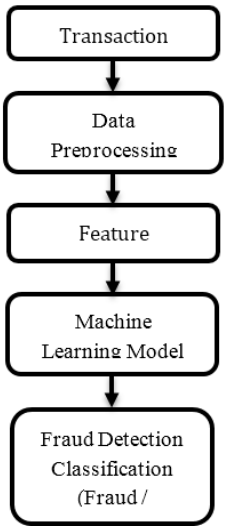

Fig. 3. Machine learning-based fraud detection workflow.

A. Performance of Fraud Detection

The fraud detection models utilized in this research show excellent results at identifying questionable financial transactions. Random Forest would be the single best performing model due to its power to analyze complex relationships among the features in the financial transaction dataset, thus giving it the highest classification accuracy of all algorithms tested. There is a similar high-performance level by neural network models at finding less obvious types of fraud, especially when looking at patterns of fraudulent transactions that are similar to those of legitimate ones. Logistic regression was able to provide both a consistent baseline for measuring the validity of the feature engineering work done and to validate the overall feature engineering process. This research presents a framework that uses multiple machine learning techniques to identify both simple and complex types of fraud in financial transaction data.

B. Impact of Multi-Layer Authentication

The use of multi-layer authentication (MLA) and device verification features greatly decrease the chances of users being able to access their accounts without authorization. By having users confirm their identity multiple times through different means, ie. through an OTP code, biometric recognition or a verified device, the ability for a user to perform a financial transaction is being narrowed to only those individuals that are authorized. Even where an attacker obtains stolen credentials via phishing or credential theft, the layers of authentication will prevent unauthorized users from accessing their financial accounts

The layered authentication creates a stronger overall security posture for digital payment services.

C. Behavioral Monitoring Analysis

The ability to engage in behavioural monitoring is a key tool for identifying potential instances of fraud that may not have been caught through typical authentication methods. The user information collected allows us to analyse transaction patterns identifying abnormal events such as transaction amounts outside of the user's historical transaction history, greater than historical transaction volume for that user as well as transaction locations outside what is typical for that user. As an example, a user, who typically performs low value transactions, suddenly initiates a number of transactions at high values within a short period of time would have their activity identified and flagged (i.e., transaction activity) for further investigation due to the high probability that it was fraudulent. Ongoing and continuous monitoring of user transaction activities increases the overall fraud detection rates and reduces the potential for an organization to incur a financial loss.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, June 2026
Impact Factor: 8.2

D. Advantages of the Proposed Framework

The new multi-layered security system has multiple benefits over conventional digital payment security systems. Listed below are five examples of these benefits.

1. Better Detection Accuracy for Fraud

By using machine-learning models, this system is capable of detecting patterns of fraud that can be difficult to detect and will detect fraud attempts that are very accurately.

2. Reduced Risk of Account Takeover

Using multi-factor authentication and identity verification features significantly decreases the chances that someone will access your accounts without your permission.

3. Ability to Monitor Transactions as They Happen

With this new system, all transactions are monitored in real time, so if a suspicious activity occurs, the transaction can be interrupted before it completes.

4. Added Security with Layers of Security

Because this new multi-layered architecture provides such a huge amount of covering security with separate forms of verification, if one layer of security fails, the other layers will still be functional to provide protection.

5. Adaptability to Newly Emerging Fraud

The fraud detection systems are based on machine learning models that can self-learn to identify new fraud patterns over time so that their systems can be kept secure for an extended period of time.

VIII. CONCLUSION

Also, digital payments are critical to modern-day financial systems because digital payments allow for secure, quick, and convenient means of conducting financial transactions over the world's digital platforms. However, with this rapid increase in the use of digital payment technology comes new cybersecurity challenges, such as identity theft, financial fraud, and unauthorized access to accounts.

Traditional authentication methods, such as passwords, PINs, and one-time passwords, will not be enough to protect individuals from sophisticated cyber-attacks.

This study proposed the development of a multi-layered security framework that integrates various authentication and fraud detection technolo gies in order to strengthen the security of digital payment systems. User authentication, multi-factor authentication, device verification, behavioral monitoring, and machine learning-based fraud detection will be combined to provide enhanced protection from fraudulent transactions.

The analysis conducted in this study demonstrates that by using different authentication methods and using intelligent fraud detection methods increases the capability of digital payment systems to identify and reject transactions based upon unusual or suspicious activity, thereby significantly enhancing the overall security against emerging cybersecurity threats. In addition, the layered security system allows for continuous monitoring and many different verification processes which will ultimately lead to increasing the overall security of digital payment systems.

This proposed structure creates new ways of providing safety & security for financial transactions using an integrated approach that combines multiple authentication methods with up-to-date methods for preventing fraudulent activities from occurring. This new design offers possible solutions to limitations associated with existing digital payment security systems that have historically separated the processes of authenticating transactions from the actual ability to detect fraudulent transactions.

Future studies may continue improving upon existing methods of protecting against digital payment fraud through exploration of innovative technologies such as blockchain technologies based on distributed ledger systems and

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, June 2026 Impact Factor: 8.2

federated machine learning algorithms used to detect fraudulent transaction activity while preserving user privacy; advanced AI-based behavioral analytics solutions capable of detecting highly sophisticated forms of digital payment fraud; and additional emerging technologies capable of increasing the scalability, privacy and intelligence aspects of digital payment security systems.

In conclusion, the multi-layered security framework described herein offers an effective option for improving overall digital payment security in response to developments within the electronic commerce marketplace.

REFERENCES

[1] M. A. Hassan, "Electronic payment systems security," Symmetry, vol. 12, 2020.
[2] V. Chang, "Digital payment fraud detection methods," Computers & Electrical Engineering, 2022.
[3] S. Aras, "Fraud detection using machine learning algorithms," 2023.
[4] M. Anderson et al., "AI-powered fraud detection in digital payments," 2026.
[5] B. Cao et al., "HitFraud: Collective fraud detection in payment networks," 2017.
[6] R. Deng and N. Ruan, "FraudJudger: Fraud detection on digital payment platforms," 2019.
[7] Z. Ke et al., "Deepfake fraud detection in online payments using GAN," 2025.
[8] A. Alabdan, "Phishing attacks survey," Future Internet, 2020.
[9] I. Akomea-Frimpong et al., "Mobile money fraud control," Journal of Money Laundering Control, 2019.
[10] P. Tran-Truong and M. Pham, "Multi-factor authentication in digital payment systems," 2025.
[11] V. R. Duvalla, "Real-time fraud detection using AI," 2025.
[12] PwC, "Combating fraud in the era of digital payments," 2023.
[13] S. Jain, "Social engineering attacks in financial systems," 2023.
[14] S. Gautam, "UPI fraud detection analysis," 2024.
[15] P. Boulieris, "Fraud detection using machine learning and NLP," 2024.
[16] IEEE, "Financial cybersecurity framework," 2021.
[17] Springer, "Digital payment security architecture," 2022.
[18] Elsevier, "Behavioral analytics for financial fraud detection," 2024.
[19] ACM, "Machine learning for financial transaction monitoring," 2023.
[20] IJPREMS, "Fraud detection using ML in digital payments," 2025.
[21] IJRAH, "Machine learning for fraud detection in payment platforms," 2024.
[22] WJARR, "Real-time AI fraud detection in financial transactions," 2025.
[23] MDPI, "Security challenges in digital financial systems," 2022.