Journal of Ubiquitous Computing and Communication Technologies (ISSN: 2582-337X)
www.irojournals.com/jucct/

Advanced Multimodal Artificial Intelligence System for Transforming Digital Banking Operations

Sowmiya M.N.[1], Amrutha C.K.[2], Beenu Sree M.[3]

Department of Information Technology, Velammal Engineering College, Chennai, India.

E-mail: [1]sowmi.rathinam93@gmail.com, [2]ckamrutha10@gmail.com, [3]2005beenusree@gmail.com

Abstract

Rapid development in the field of digital banking systems has brought to light a lot of problems related to security, fraud detection, and effective finance management. The currently available approaches are based on the use of the existing solutions, which cannot address the modern trends in the field of cyber threats and fraudulent attacks. The purpose of this project is to develop a reliable transaction system with the aid of authentication and machine learning-based fraud detection. PIN identification and facial recognition will be used to ensure the authentication of the user before executing any transaction. To run the experiment, 50,000 synthetic transactions characterized by the value of each transaction, its time interval, and transaction frequency will be created. Anomaly detection is performed using an isolation forest machine learning algorithm through Scikit-learn to detect abnormal transactions without having to label them. The overall architecture of the system comprises a user module, an admin module, and MySQL database backend for storage and monitoring purposes.

Keywords: Digital Banking, Fraud Detection, Machine Learning, Anomaly Detection, Financial Security, Intelligent Banking Systems, Biometric Authentication, Automation

1. Introduction

The fast development of digital technology has revolutionized the banking industry by bringing about speedy and secure transactions as well as financial convenience. The use

DOI: https://doi.org/10.36548/jucct.2026.2.003
Received: 23.02.2026, received in revised form:26.03.2026, accepted: 14.04.2026, published: 25.04.2026

of online and mobile banking services has resulted in a surge in digital money transactions. This is not without its difficulties since there is a need for security, fraud detection, and effective management of funds in order to facilitate these transactions. Due to increasing threats from cyber-attacks and fraud, there is a need to develop reliable security systems [1], [7].

The conventional fraud detection systems used in banks depend on rule-based methods and manual analysis methods. The problem with such systems is that while they work well with known fraud scenarios, they cannot cope with new emerging forms of fraud within a huge and high dimensional set of data. This has created the need to develop automated systems that are capable of detecting any form of anomaly in transactions and subsequently detect any fraud. Machine Learning models have proved to be useful in detecting anomalies and hence fraud without necessarily labeling the dataset [1], [2]. The system is suitable in environments where fraud is uncommon and evolves over time.

Apart from fraud prevention, another critical issue that exists in online banking systems is user authentication. Traditional password-based user authentication can be subject to a number of attacks including phishing and credential attacks. In order to counteract the above shortcomings, biometric user authentication techniques such as facial recognition have received much focus recently due to their improved security features [6].

In response to these issues, this research proposes the Advanced Multimodal Artificial Intelligence System for innovation in digital banking transaction processes. This proposed system will implement different intelligent systems, including the fraud detection system based on anomalies, the multimodal authentication method with PIN and facial recognition technology, and the transaction monitoring process. Also, this system will have different user and administrator modules through the MySQL database system.

The main contributions of this work are as follows:

- Development of a multimodal AI-based digital banking framework
- Implementation of unsupervised fraud detection using Isolation Forest
- Integration of PIN-based and biometric authentication for enhanced security
- Real-time transaction monitoring and anomaly detection

- Design of a scalable architecture with user and admin control modules

2. Literature Review

The evolution of digital banking has greatly benefited from innovations in AI technologies such as fraud detection, security, and user experiences. Anomaly detection is one of the critical components in discovering abnormal behaviors within the financial transactions. In [1], a complete review of different anomaly detection approaches is discussed, with great attention being paid to their application in the detection of frauds. In [2], an efficient isolation forest method was proposed to effectively isolate anomalies in high-dimensional data spaces, which makes it possible to detect fraud in a real-time financial environment.

In [3], the use of ADASYN with feature selection and cross-validation helps achieve enhanced results when developing models for credit card fraud detection. Besides, there is an effective framework for streaming fraud detection that uses big data technology, as shown in [4]. Thus, one should note that the mentioned techniques require a combination of various models and methods to be able to process the data. One of the most popular models today is deep learning, which serves as a basis for intelligent banking systems. As explained in [5], the main principles of deep learning enable the development of efficient solutions based on neural networks for risk assessment and prediction.

In addition, multimodal deep learning allows the merging of diverse types of information such as transaction data, customer behavior data, and textual data in an effort to improve the overall functioning of the AI systems. Multi-modal AI systems utilizing various sources of data can significantly benefit from this approach. Moreover, it is important to note that security measures as well as user authentication are necessary for the smooth running of digital banking systems. As noted in [6], biometric identification systems can be useful in providing an effective mechanism for user authentication and avoiding threats associated with password use.

The development of finance technologies is analyzed in [8], where the transition from traditional to digitized and technology-based banking services due to worldwide economic shifts is discussed. Such development has laid a groundwork for the implementation of sophisticated AI solutions in banks. Also, the significance of AI for operational optimization, client service enhancement, and fraud prevention in banks is noted in [10].

In summary, the literature shows that the incorporation of anomaly detection, machine learning, deep learning, biometric authentication, and blockchain technology serves as the backbone for advanced multimodal AI systems. Such a combination of methods helps digital banks become more secure and capable of making decisions.

3. Methodology

Below figure 1 demonstrates the overall structure of the system being developed, which includes the user module, authentication module, machine learning module, decision-making module, administrative module, and database module.

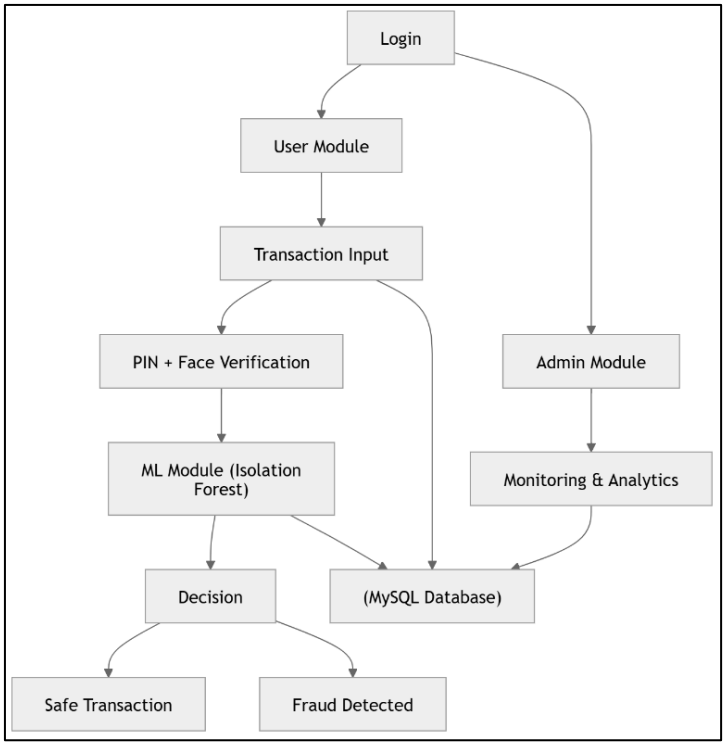

Figure 1. System Architecture of the Proposed Multimodal AI-Based Digital Banking System

3.1 User Module

User module plays the role of launching and coordinating activities of the user within the system. Through this module, a user gains access into the system through logging in, choosing his/her bank account, and then inputting the required details about the transactions like transaction amount, interval period, frequency, and recipient details among others. This module has been made in a user-friendly way so that transactions are conducted easily and

the users are not bothered by the complexities of the back-end. After all this is done, the data is passed on to the authentication module for verification purposes.

3.2 Authentication Module (PIN and Facial Recognition)

The Authentication Module is a two-factor security model because it uses the combination of verifying a PIN and performing biometric authentication. In the beginning, the user has to enter a 4-digit PIN number, which is then validated with the credentials from the database. Once the validation of the PIN number is successful, the facial verification takes place via the camera module. The face of the user is scanned and verified with the registered face images. These two stages help minimize the probability of any fraud or unauthorized access.

3.3 Machine Learning Module (Fraud Detection using Isolation Forest)

The machine learning technique serves as the key factor for the detection of fraud transactions in our solution. The function carried out by the machine learning module entails receiving raw transaction data as input, passing it through a sequence of procedures, and generating outputs that notify the user and administrator of irregularities in their transactions.

Following figure 2 presents the step-by-step workflow of transaction processing.

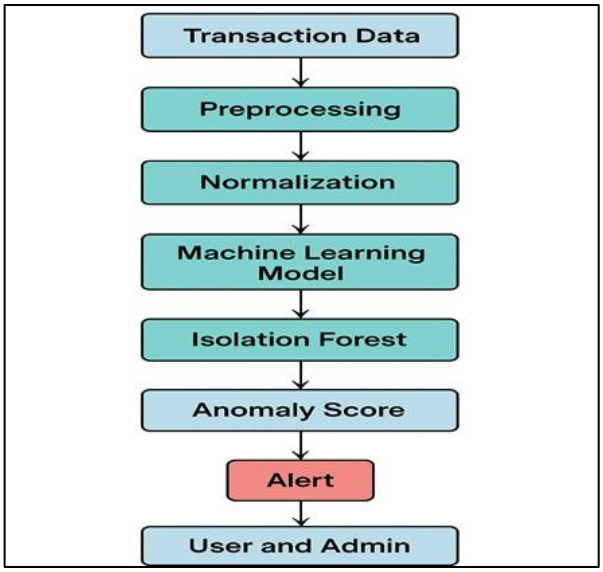

Figure 2. Workflow of Secure Transaction Processing

Initially, the transaction data that are to be analyzed are collected. These data points encompass the amount of transactions, the gap between the transactions, the rate of the

transactions, and others. These features are determined based on their capability to reflect particular traits of the transaction, whether it is fraudulent or legitimate. For our solution, we utilize artificial data with 50,000 transactions. These data points are created to mirror the activities of individuals under realistic conditions. After collecting the required data, preprocessing becomes the subsequent task carried out. Preprocessing is focused on dealing with discrepancies such as missing data and noise in order to guarantee high-quality data in the data set.

The normalized value of the features is obtained following the preprocessing stage where the data is normalized in order to bring all the feature values within the same range. It is vital that this be done since the transactions' features such as the amount and frequency could have very different ranges. Through normalization, we make sure that there is no particular feature that would dominate the other features in terms of influence and hence improve accuracy and stability. The normalized data will then be fed to the machine learning model which will use the Isolation Forest algorithm. The Isolation Forest uses the unsupervised learning method to detect anomalies. Due to their uniqueness, the fraudulent transactions will be isolated very fast, hence scoring higher on the anomaly scale than other types of transactions.

Once the model processes the data, the algorithm will assign an anomaly score to each transaction. This score will represent numerically the probability that the transaction is fraudulent. The lower the score, the less probable the transaction is to be fraudulent, but when the score is high, there could be some anomaly present. A defined anomaly threshold helps us define whether a transaction is legitimate or fraudulent. Whenever the anomaly score is higher than the threshold, an alert will be generated, implying that a possible fraudulent act occurred. The alerting process is of utmost importance since it helps prevent fraud by taking immediate action. Such alerts are sent to the user and admin modules.

The whole process provides an uninterrupted transition from collecting raw data to making informed decisions. Combining preprocessing, normalization, and the Isolation Forest algorithm helps to detect fraudulent transactions accurately and efficiently on a large scale. Due to the capability to find unknown fraud patterns and make instant decisions, the proposed approach is applicable in real-world scenarios.

3.4 Decision Module

The Decision Module serves as the ultimate decision-making component within the transaction procedure. The module makes its decision based on the outcome produced by the machine learning algorithm and then decides whether the transaction must be allowed or denied. In cases where the transaction turns out to be legitimate, the module allows the transaction to take place, resulting in a successful transfer of funds. On the other hand, when the transaction turns out to be fraudulent, the module denies the transaction.

3.5 Admin Module

The Admin Module is responsible for system-wide monitoring, management, and analysis of data. Through this module, the administrator will be able to access information about the users that have been registered, manage their accounts, and examine transactional data in the database. Furthermore, the module will give fraud detection information and system evaluation measures including accuracy, precision, recall, and F1 score. Through this module, administrators are able to analyze system data and identify any suspicious behavior, if there is any, and handle the situation appropriately.

3.6 Database Layer

The Database Layer is developed with the help of MySQL and acts as a central location to store all the data of the system. This includes login credentials, facial data of customers, transaction information, and information related to the fraud detection process. This database is helpful in ensuring that data retrieval becomes easy and facilitates real-time communication between various components of the system.

The whole system works sequentially, from the start of the transaction to its completion or blocking, depending on the results of the work performed. First of all, the user makes an attempt to make a payment, and the transaction is verified using PIN code and face recognition. After that, when a transaction passes the security check and is confirmed, data about the transaction is processed with the help of the machine learning algorithm to find out whether the transaction is fraudulent. All actions are recorded in the database and controlled via the administrator console.

4. Results and Discussion

Performance Evaluation of the Proposed Fraud Detection Model A performance evaluation of the proposed fraud detection model is conducted on an artificially generated dataset, which comprised of 50,000 transactions. Both legitimate and fraudulent transactions were combined to resemble the real-world scenario, including key transaction characteristics such as transaction amount, the time gap between transactions, and the frequency of the transactions. Table 1 presents a subset of the synthetic transaction dataset used for model training and testing.

Table 1. Sample Representation of Synthetic Transaction Dataset

Transaction ID	Amount (₹)	Time Interval (sec)	Frequency	Label
T001	250	30	2	Genuine
T002	12,500	5	8	Fraud
T003	1,200	60	1	Genuine
T004	45,000	2	12	Fraud
T005	800	120	1	Genuine

The developed model was based on the Isolation Forest algorithm since this type of model fits best for anomaly detection tasks that do not involve the use of labeled data. For testing the generalizability of the created model, the dataset was split in 80:20. For creating the model and visualizing its output, the following tools were used: Python with Scikit-learn, MySQL, and Streamlit.

Table 2. Experimental Setup of the Proposed System

Parameter	Value / Description
Total Transactions	50,000
Genuine Transactions	47,500 (95%)
Fraudulent Transactions	2,500 (5%)

Training Data Size	40,000 (80%)
Testing Data Size	10,000 (20%)
Algorithm Used	Isolation Forest
Learning Type	Unsupervised Learning
Key Features Considered	Transaction Amount, Time Interval, Frequency
Tools & Technologies	Python, Scikit-learn, MySQL, Streamlit
Evaluation Metrics	Accuracy, Precision, Recall, F1-Score

Figure 3. Sample Dashboard for the Proposed System

Figure 3 shows the user interface dashboard employed to monitor transactions, fraud alerting messages and system performance statistics on real-time basis.

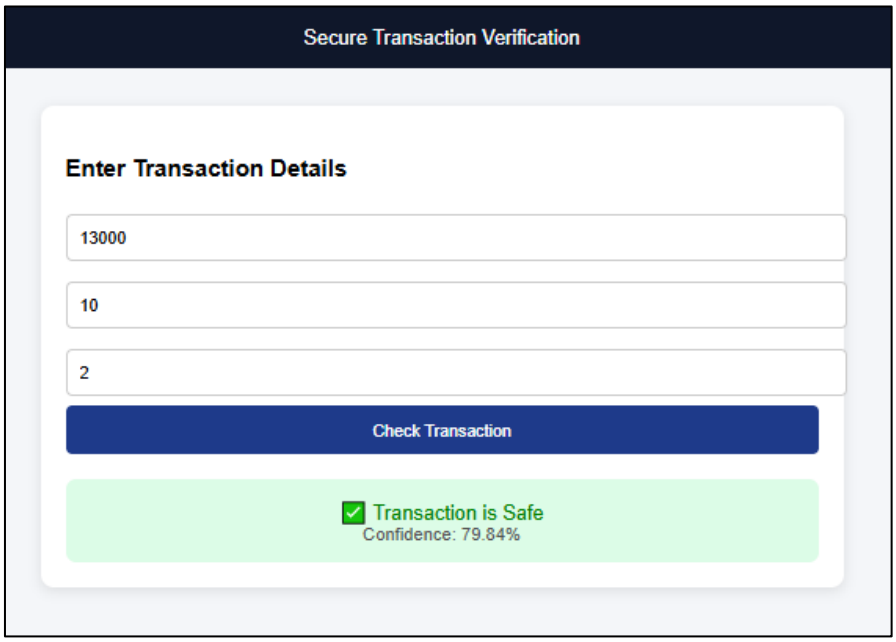

Figure 4. Sample Screen of Safe Transaction

Above figure 4 depicts the output of the system when a transaction has been authenticated as genuine or legitimate. Figure 5 shows the response of the system when a fraudulent transaction is detected.

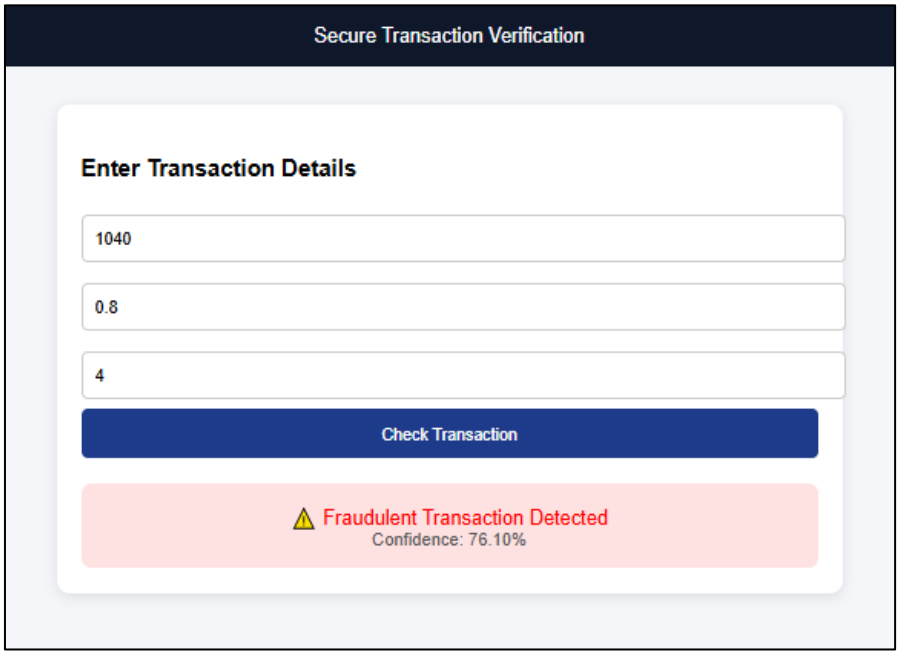

Figure 5. Sample Screen of Fraudulent Transaction

As seen below in table 3, there is a quantification of the performances achieved by the proposed model through standard performance evaluation measures.

Table 3. Performance Evaluation Metrics of the Proposed Fraud Detection System

Metric	Value
Accuracy	0.981
Precision	0.968
Recall	0.935
F1-Score	0.926

The anomaly detection performed using the Isolation Forest method was done successfully since good precision was achieved. The high accuracy of detection meant that very few legitimate users would be wrongly classified. Additionally, this algorithm showed great flexibility in detecting new cases of fraud.

Table 4. Comparative Analysis of Authentication Mechanisms

Method	Accuracy	Average Time
Password-Based	0.82	1.2 sec
Facial Recognition (LBPH)	0.954	1.8 sec
Proposed Multimodal System	0.981	2.1 sec

Table 4 compares various authentication techniques in terms of their accuracy and average processing time. It shows the enhanced performance of the proposed multimodal authentication system compared to the conventional password-based and face recognition techniques.

Table 5. System Efficiency Metrics

Parameter	Value
Transaction Processing Time	0.45 sec
Fraud Detection Time	0.12 sec

System Response Time	< 1 sec

Table 5 represents performance metrics of system at system level, such as the time taken to process transactions, the time required for fraud detection, and the total response time of system.

The integration of facial recognition with passwords enhances security. Even if the authentication process takes longer than usual, the advantages far outweigh the disadvantages because there will be more accuracy and improved security. This type of system will almost be in real time, making its application in practice relatively easy.

5. Conclusion

The proposed system effectively proves that a viable architecture can be implemented for secure transaction processing through a combination of authentication and machine learning fraud detection. The use of both PIN authentication and face recognition helps to authenticate users, thereby preventing any access from unauthorized persons. The use of Isolation Forest algorithm facilitates the detection of fraud through the identification of all the new patterns of fraud without the use of labeled data. From experiments conducted using synthetic transaction data totaling 50,000 transactions, high levels of accuracy and precision were achieved with a very low percentage of false positives. In terms of architecture, the system has a modulated structure comprising both user and administrator interfaces backed by MySQL database server. Even though the process takes a little more time for authentication, the improved security aspect makes up for it.

References

[1] Chandola, Varun, Arindam Banerjee, and Vipin Kumar. "Anomaly Detection: A Survey." ACM computing surveys (CSUR) 41, no. 3 (2009): 1-58.

[2] Liu, Fei Tony, Kai Ming Ting, and Zhi-Hua Zhou. "Isolation Forest." In 2008 Eighth IEEE International Conference on Data Mining, 2008, 413-422.

[3] Ileberi, Emmanuel, and Yanxia Sun. "Advancing Model Performance with ADASYN and Recurrent Feature Elimination and Cross-Validation in Machine Learning-Assisted

Credit Card Fraud Detection: A comparative analysis." IEEE access 12 (2024): 133315-133327.

[4] Carcillo, Fabrizio, Andrea Dal Pozzolo, Yann-Aël Le Borgne, Olivier Caelen, Yannis Mazzer, and Gianluca Bontempi. "Scarff: A Scalable Framework for Streaming Credit Card Fraud Detection with Spark." Information fusion 41 (2018): 182-194.

[5] Goodfellow, Ian, Yoshua Bengio, Aaron Courville, and Yoshua Bengio. Deep Learning. Vol. 1, no. 2. Cambridge: MIT press, 2016, 1-800.

[6] Jain, Anil K., Arun Ross, and Salil Prabhakar. "An Introduction to Biometric Recognition." IEEE Transactions on circuits and systems for video technology 14, no. 1 (2004): 4-20.

[7] Kshetri, Nir. "Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy." Telecommunications policy 41, no. 10 (2017): 1027-1038.

[8] Arner, Douglas W., Janos Barberis, and Ross P. Buckley. "The Evolution of Fintech: A New Post-Crisis Paradigm." Geo. J. Int'l L. 47 (2015): 1271.

[9] Ngiam, Jiquan, Aditya Khosla, Mingyu Kim, Juhan Nam, Honglak Lee, and Andrew Y. Ng. "Multimodal Deep Learning." In Icml, vol. 11, 2011, 689-696.

[10] Sharma, Priya. "Transforming Banking Through Artificial Intelligence: Enhancing Service, Efficiency, and Security for the Digital Age." International Journal of Science and Technology (IJST) 1, no. 4 (2024): 10-21.